103D CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 103–601
Part 5

pt.5

HEALTH SECURITY ACT

AUGUST 12, 1994.—Ordered to be printed

Mr. CONYERS, from the Committee on Government Operations, submitted the following

REPORT

[To accompany H.R. 3600 which on November 20, 1993, was referred jointly to the Committee on Energy and Commerce, to the Committee on Ways and Means, and to the Committee on Education and Labor for consideration of such provisions in titles I, III, VI, VIII, X, and XI and part 1 of subtitle C of title V as fall within its jurisdiction pursuant to clause 1(g) of rule X; and concurrently, for a period ending not later than two weeks after all three committees of joint referral report to the House (or a later time if the Speaker so designates), to the Committee on Armed Services for consideration of subtitle A of title VIII and such provisions of title I as fall within its jurisdiction pursuant to clause 1(c) of rule X, to the Committee on Veterans' Affairs for consideration of subtitle B of title VIII and such provisions of title I as fall within its jurisdiction pursuant to clause 1(u) of rule X, to the Committee on Post Office and Civil Service for consideration of subtitle C of title VIII and such provisions of title I as fall within its jurisdiction pursuant to clause 1(o) of rule X, to the Committee on Natural Resources for consideration of subtitle D of title VIII and such provisions of title I as fall within its jurisdiction pursuant to clause 1(n) of rule X, to the Committee on the Judiciary for consideration of subtitles C through F of title V and such other provisions as fall within its jurisdiction pursuant to clause 1(l) of rule X, to the Committee on Rules for consideration of sections 1432(d), 6006(f), and 9102(e)(5), and to the Committee on Government Operations for consideration of subtitle B of title V and section 5401]

The Committee on Government Operations, to whom was referred the bill (H.R. 3600) to ensure individual and family security through health care coverage for all Americans in a manner that contains the rate of growth in health care costs and promotes responsible health insurance practices, to promote choice in health care, and to ensure and protect the health care of all Americans,

82–256

having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

CONTENTS

Page 859, strike lines 16 through 18 and insert the following (and conform the table of contents of title V accordingly):

Subtitle B—Administrative Simplification and Fair Health Information Practices

Amend part 1 of subtitle B of title V (page 859, line 19, through page 870, line 23) to read as follows (and redesignate provisions and conform the table of contents of title V accordingly):

PART 1—ADMINISTRATIVE SIMPLIFICATION STANDARDS

SEC. 5101. PURPOSE.

It is the purpose of this part to improve the efficiency and effectiveness of the health care system by encouraging the development of a health information network through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 5102. DEFINITIONS.

For purposes of this part:

(1) CARRIER.—The term "carrier" means a licensed insurance company, a hospital or medical service corporation (including an existing Blue Cross or Blue Shield organization, within the meaning of section 833(c)(2) of the Internal Revenue Code of 1986), a health maintenance organization, or other entity licensed or certified by a State to provide health insurance or health benefits.

(2) CODE SET.—The term "code set" means any set of codes used for encoding data elements of health information, including tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

(3) COORDINATION OF BENEFITS.—The term "coordination of benefits" means determining and coordinating the financial obligations of health information plan

sponsors when health care benefits are payable under two or more such plans.

(4) HEALTH INFORMATION.—The term "health information" means any information that relates to the past, present, or future physical or mental health or condition or functional status of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual.

(5) HEALTH INFORMATION NETWORK.—The term "health information network" means the health information system that is formed through the application of the requirements of, and the standards established under, this part.

(6) HEALTH INFORMATION NETWORK SERVICE.—The term "health information network service"—

(A) means a private entity or an entity operated by a State that enters into contracts—

(i) to process or facilitate the processing of nonstandard health information into standard health information;

(ii) to provide the means by which persons are connected to the health information network for purposes of meeting the requirements of this part;

(iii) to provide authorized access to health information through the health information network; or

(iv) to provide specific information processing services, such as automated coordination of benefits and claims transaction routing; and

(B) includes a health information protection organization.

(7) HEALTH INFORMATION PLAN.—

(A) IN GENERAL.—The term "health information plan" means—

(i) any contract of health insurance, including any hospital or medical service policy or certificate, hospital or medical service plan contract, or health maintenance organization group contract, that is provided by a carrier; and

(ii) an employee welfare benefit plan or other arrangement insofar as the plan or arrangement provides health benefits and is funded in a manner other than through the purchase of one or more policies or contracts described in clause (i).

(B) EXCEPTION.—The term "health information plan" does not include any of the following (or any combination thereof):

(i) Coverage issued as a supplement to liability insurance.

(ii) Liability insurance, including general liability insurance and automobile liability insurance.

(iii) Worker's compensation or similar insurance.

(iv) Automobile medical-payment insurance.

(8) HEALTH INFORMATION PLAN SPONSOR.—The term "health information plan sponsor" means—

(A) a carrier or an eligible sponsor (as defined in section 1311(b)) providing a health plan; and

(B) a carrier or other person providing any other health information plan, including any public entity that provides payments for health care items and services under a health information plan that are equivalent to payments provided by a private person under such a plan.

(9) HEALTH INFORMATION PROTECTION ORGANIZATION.—The term "health information protection organization" means a private entity or an entity operated by a State that accesses standard health information through the health information network and processes such information into standard non-identifiable health information.

(10) HEALTH SERVICE PROVIDER.—The term "health service provider" means a provider of services (as defined in section 1861(u) of the Social Security Act), a physician, a laboratory (as defined in section 353(a) of the Public Health Service Act), a supplier, and any other person furnishing health care. Such term includes a Federal or State program that directly provides items or services that constitute health care to beneficiaries.

(11) NON-IDENTIFIABLE HEALTH INFORMATION.—The term "non-identifiable health information" means health information that is not protected health information.

(12) PATIENT MEDICAL RECORD INFORMATION.—The term "patient medical record information" means health information derived from a clinical encounter that relates to the past, present, or future physical or mental health or condition or functional status of an individual.

(13) PROTECTED HEALTH INFORMATION.—The term "protected health information" has the meaning given such term in section 5120(a)(3).

(14) STANDARD.—The term "standard", when used with reference to health information or a transaction involving such information, means that the information or transaction meets any standard established by the Secretary under section 5103 that applies to the information or transaction.

Subpart A—Standards and Requirements With Respect to Health Information, Information Transactions, and Health Information Network Services

SEC. 5103. STANDARDS FOR HEALTH INFORMATION AND INFORMATION TRANSACTIONS.

(a) STANDARDS TO ENSURE COMPARABILITY OF INFORMATION.—

(1) IN GENERAL.—The Secretary shall establish standards necessary to make a set of health information described in subsection (b) that is created by a health information plan sponsor or a health service provider comparable with the same set of information created by another such sponsor or provider.

(2) DATA ELEMENTS.—The standards shall specifically define the data elements that comprise each set of health information described in subsection (b).

(3) FORMAT.—The standards shall include uniform presentation and format requirements for the arrangement of data elements.

(4) ELECTRONIC.—The standards shall require that health information be in electronic or magnetic form.

(5) UNIQUE IDENTIFIERS.—The Secretary shall establish a system to provide for a unique identifier for each eligible individual, employer, health information plan, health information plan sponsor, and health service provider.

(6) CODE SETS.—The Secretary, in consultation with experts from the private sector and Federal agencies—

(A) shall select code sets for appropriate data elements from among the code sets that have been developed by private and public entities; or

(B) shall establish code sets for appropriate data elements if no code set for the data elements has been developed by such entities.

(b) SETS OF HEALTH INFORMATION.—

(1) PLAN AND PROVIDER TRANSACTIONS.—The Secretary shall establish a separate set of health information that is appropriate for transmission in connection with each transaction described in subsections (a) and (b) of section 5104.

(2) ENCOUNTER INFORMATION.—The Secretary shall establish a set of encounter information (including patient medical record information) derived from inpatient and outpatient clinical encounters that the Secretary determines—

(A) is appropriate for creation by a health service provider to the extent the sponsor does not file claims for reimbursement for items and services with health information plan sponsors; and

(B) is necessary to provide information regarding the operation of such a health service pro-

vider, and health-related items and services provided by the provider, that is equivalent to information derived from claims.

(3) PATIENT MEDICAL RECORD INFORMATION.—The Secretary shall establish a set of patient medical record information.

(4) ADDITIONS TO SETS.—The Secretary may make additions to a set of health information established under paragraph (1), (2), or (3) as the Secretary determines appropriate in a manner that minimizes the disruption to, and costs of compliance incurred by, a health information plan sponsor or a health service provider that is required to comply with section 5104.

(c) STANDARDS FOR INFORMATION TRANSACTIONS.—The Secretary shall establish standards relating to technical aspects of the procedure, method, and mode by which a health information plan sponsor or a health service provider that is required to comply with section 5104 may transmit electronically under section 5104 health information that is included in a set of health information described in subsection (b). The standards shall include standards with respect to the format in which such information shall be transmitted under such section.

(d) GENERAL REQUIREMENTS.—In establishing standards under this section, the Secretary shall, to the maximum extent practicable—

(1) require the use of information that is verifiable, timely, accurate, reliable, useful, and relevant;

(2) establish standards that are consistent with the objective of reducing the costs of providing and paying for health care;

(3) incorporate standards that are in use and generally accepted, or developed, by standard setting or standard development organizations, including the American National Standard Institute Federation and the Healthcare Informatics Standards Planning Panel; and

(4) rely on and cooperate with organizations described in paragraph (3).

(e) TIMETABLES FOR STANDARDS.—

(1) INITIAL STANDARDS.—

(A) IN GENERAL.—The Secretary shall develop an expedited process for the establishment of initial standards under this section.

(B) STANDARDS TO ENSURE COMPARABILITY OF INFORMATION.—

(i) IN GENERAL.—Except as provided in clause (ii), not later than 9 months after the date of the enactment of this Act, the Secretary shall establish standards under subsection (a) with respect to each set of health information described in subsection (b).

(ii) EXCEPTIONS.—Not later than 24 months after the date of the enactment of this Act,

the Secretary shall establish standards under subsection (a) with respect to health information that is appropriate for transmission in connection with the submission of a claim attachment and the set of patient medical record information established under subsection (b)(3). The Secretary shall establish standards under subsection (a) with respect to health information that is added to a set of health information under subsection (b)(4) in conjunction with making such addition.

(C) STANDARDS FOR INFORMATION TRANSACTIONS.—

(i) IN GENERAL.—Except as provided in clause (ii), the Secretary shall establish standards under subsection (c) not later than 9 months after the date of the enactment of this Act.

(ii) EXCEPTION.—Not later than 24 months after the date of the enactment of this Act, the Secretary shall establish standards under subsection (c) with respect to the submission of a claim attachment.

(2) MODIFICATIONS TO STANDARDS.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the Secretary shall review the standards established under this section and shall modify such standards as determined appropriate, but not more frequently than once every 6 months. Any modification under this subparagraph shall be made in a manner that minimizes the disruption to, and costs of compliance incurred by, a health information plan sponsor or a health service provider that is required to comply with section 5104.

(B) SPECIAL RULES.—

(i) MODIFICATIONS DURING FIRST 12-MONTH PERIOD.—The Secretary may not modify a standard established under this section during the 12-month period beginning on the date the standard is established unless the Secretary determines that a modification is necessary in order to permit a health information plan sponsor or a health service provider to comply with section 5104.

(ii) ADDITIONS AND MODIFICATIONS TO CODE SETS.—

(I) IN GENERAL.—The Secretary shall ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets to accommodate changes in biomedical science and health care delivery.

(II) ADDITIONAL RULES.—If a code set is modified under this clause, the modified code set shall include instructions on how data elements that were encoded prior to the modification are to be converted or translated so as to preserve the value of the data elements. Any modification to a code set under this subsection shall be implemented in a manner that minimizes the disruption to, and costs of compliance incurred by, a health information plan sponsor or a health service provider that is required to comply with section 5104.

(f) EVALUATION OF STANDARDS.—The Secretary may establish a process to measure or verify the consistency of standards established or modified under this section. The process may include demonstration projects and analysis of the cost of implementing such standards and modifications.

(g) DISTRIBUTION OF CODE SETS.—The Secretary shall establish efficient and low-cost procedures for the distribution of code sets that are selected, established, or modified under this section.

SEC. 5104. REQUIREMENTS ON PLANS AND PROVIDERS.

(a) TRANSACTIONS BY PLANS AND PROVIDERS.—

(1) IN GENERAL.—If a health information plan sponsor conducts any of the transactions described in paragraph (2) with a health service provider, the transaction shall be a standard transaction and the health information transmitted or received in connection with the transaction shall be standard health information.

(2) TRANSACTIONS.—The transactions referred to in paragraph (1) are the following:

(A) Claim submission.

(B) Submission of claim attachments.

(C) Coordination of benefits.

(D) Such other transactions required under this Act or determined appropriate by the Secretary as the Secretary may specify consistent with the goal of reducing administrative costs.

(b) TRANSACTIONS BY PLANS.—

(1) IN GENERAL.—If a health information plan sponsor conducts any of the transactions described in paragraph (2) with any person (other than an individual acting in the capacity of an eligible individual or a consumer of health care services), the transaction shall be a standard transaction and the health information transmitted or received by the sponsor in connection with the transaction shall be standard health information.

(2) TRANSACTIONS.—The transactions referred to in paragraph (1) are the following:

(A) Enrollment and disenrollment.

(B) Eligibility verification.

(C) Payment and remittance advice.

(D) Claims status verification.

(E) Certification or authorization of a referral to a health service provider who is not a member of a provider network of the health information plan provided or sponsored by the sponsor.

(F) Such other transactions required under this Act or determined appropriate by the Secretary as the Secretary may specify consistent with the goal of reducing administrative costs.

(c) DISCLOSURE OF INFORMATION.—

(1) IN GENERAL.—A health information plan sponsor or a health service provider shall have the capacity to make the standard health information transmitted or received by the sponsor or provider in connection with standard transactions described in subsections (a)(2) and (b)(2), or acquired by the sponsor or provider pursuant to section 5108(a), available for disclosure as authorized under section 5105 and part 2.

(2) SPECIAL RULE.—To the extent that a health service provider does not file claims for reimbursement for items and services with health information plan sponsors, the provider shall have the capacity to make standard health information regarding the items and services that is included in the set of encounter data established by the Secretary under section 5103(b)(2) available for disclosure as authorized under section 5105 and part 2.

(d) USE OF HEALTH INFORMATION NETWORK SERVICES.—A health information plan sponsor or a health service provider may comply with any provision of this section by entering into an agreement or other arrangement with a health information network service certified under section 5107 pursuant to which the service undertakes the duties applicable to the sponsor or provider under the provision.

(e) TIMELINESS.—A health information plan sponsor or a health service provider shall be considered to have satisfied a requirement under this section only if any action required to be taken by the sponsor or provider under the requirement is completed in a timely manner, as determined under standards established by the Secretary. In setting standards under this subsection, the Secretary shall take into consideration—

(1) the age and amount of the health information to which the requirement pertains; and

(2) the ability of a sponsor or provider to comply with the requirement.

(f) TIMETABLES FOR COMPLIANCE.—

(1) INITIAL COMPLIANCE.—

(A) IN GENERAL.—Not later than 12 months after the date on which standards are established under section 5103 with respect to a transaction referred to in subsection (a)(1) or (b)(1) or a set of health information described in section 5103(b), a

health information plan sponsor or health service provider shall comply with the requirements of this section with respect to the transaction or information.

(B) ADDITIONAL HEALTH INFORMATION.—Not later than 12 months after the date on which the Secretary makes an addition to a set of health information under section 5103(b), a health information plan sponsor or health service provider shall comply with the requirements of this section with respect to the additional information.

(2) COMPLIANCE WITH MODIFIED STANDARDS.—

(A) IN GENERAL.—If the Secretary modifies a standard established under section 5103, a health information plan sponsor or health service provider shall comply with the modified standard at such time as the Secretary determines appropriate, taking into account the nature and intent of the modification.

(B) SPECIAL RULE.—In the case of a modification to a standard under subparagraph (A) that does not occur within the 12-month period beginning on the date the standard is established, the time determined appropriate by the Secretary under subparagraph (A) may not be—

(i) earlier than the last day of the 90-day period beginning on the date the modified standard is established; or

(ii) later than the last day of the 12-month period beginning on the date the standard is established.

SEC. 5105. ACCESSING HEALTH INFORMATION.

(a) ACCESS FOR AUTHORIZED PURPOSES.—The Secretary shall establish standards under which appropriate persons, including health information plan sponsors, health service providers, health information network services, and Federal and State agencies, may locate and access standard health information described in section 5104(c) through the health information network. The standards shall include safeguards to ensure that a person requesting health information is authorized under part 2 to receive the information.

(b) ACCESS BY FEDERAL AND STATE AGENCIES.—A health information protection organization that is certified under section 5107 shall make available to a Federal or State agency pursuant to a cost-type contract (as defined under the Federal Acquisition Regulation) any standard health information described in section 5104(c) that—

(1) is requested by the agency; and

(2) both the agency and the organization are authorized to receive under part 2.

(c) ACCESS BY HEALTH INFORMATION PROTECTION ORGANIZATIONS.—If a health information protection organization that is certified under section 5107 requires health in-

formation from a health information plan sponsor or a health service provider in order to comply with a request by a Federal or State agency under subsection (b) that is made to fulfill a requirement under this Act, the sponsor or provider shall make the information available to the organization at no charge.

(d) LENGTH OF TIME INFORMATION ACCESSIBLE.—The Secretary shall establish standards with respect to the length of time any data element in a set of health information established under section 5103(b) should be available through the health information network under this section.

(e) USE OF HEALTH INFORMATION NETWORK SERVICES.—A health information plan sponsor or a health service provider may comply with any provision of this section by entering into an agreement or other arrangement with a health information network service certified under section 5107 pursuant to which the service undertakes the duties applicable to the sponsor or provider under the provision.

(f) TIMETABLES FOR STANDARDS AND COMPLIANCE.—

(1) INITIAL STANDARDS.—The Secretary shall establish standards under this section not later than 9 months after the enactment of this Act and such standards shall be effective upon establishment.

(2) MODIFICATIONS TO STANDARDS.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the Secretary shall review the standards established under this section and shall modify the standards as determined appropriate, but not more frequently than once every 6 months. Any modification under this subparagraph shall be made in a manner that minimizes the disruption to, and costs of compliance incurred by, a health information plan sponsor or a health service provider that is required to comply with section 5104. Any modification to a standard under this section shall be effective upon establishment.

(B) SPECIAL RULE.—The Secretary may not modify any standard under this section during the 12-month period beginning on the date the standard is established unless the Secretary determines that a modification is necessary in order to permit a health information plan sponsor or a health service provider to comply with this section or section 5104(c).

SEC. 5106. PROTECTION OF COMMERCIAL INFORMATION.

In establishing standards under this part, the Secretary shall not require disclosure of trade secrets and confidential commercial information by entities operating in the health information network except as required under a law other than this Act.

SEC. 5107. STANDARDS AND CERTIFICATION FOR HEALTH INFORMATION NETWORK SERVICES.

(a) STANDARDS FOR OPERATIONS.—The Secretary shall establish standards with respect to the operation of health information network services, including standards ensuring that such services—

(1) develop, operate, and cooperate with one another to form a health information network;

(2) meet all of the requirements under part 2 that are applicable to such services;

(3) make public information concerning their performance, as measured by uniform indicators such as accessibility, transaction responsiveness, administrative efficiency, reliability, dependability, and any other indicator determined appropriate by the Secretary; and

(4) have the highest security procedures that are practicable with respect to the processing and handling of health information.

(b) CERTIFICATION BY SECRETARY.—

(1) ESTABLISHMENT OF PROCEDURE.—Not later than 12 months after the date of the enactment of this Act, the Secretary shall establish a certification procedure for health information network services which ensures that services certified under this section are qualified—

(A) to meet the requirements of this part and the standards established by the Secretary under this section; and

(B) to ensure the confidentiality of protected health information as required under part 2.

(2) DEEMED CERTIFICATION.—The Secretary may designate private individuals or entities to conduct the certification procedure established by the Secretary under this subsection. A health information network service certified by such an individual or entity in accordance with such designation shall be considered to be certified by the Secretary under this subsection.

(3) APPLICATION FOR CERTIFICATION.—Each entity desiring to be certified as a health information network service shall apply to the Secretary for certification in a form and manner determined appropriate by the Secretary.

(4) AUDITS AND REPORTS.—The procedure established under paragraph (1) shall provide for audits by the Secretary and reports by an entity certified under this section as the Secretary determines appropriate in order to monitor the compliance by the entity with the requirements of this part and the standards established by the Secretary under this section.

(5) RECERTIFICATION.—A health information network service shall be recertified under this subsection not less than every 3 years.

(c) LOSS OF CERTIFICATION.—

(1) MANDATORY TERMINATION.—If a health information network service violates a provision of part 2, the certification of the service under this section shall be terminated unless the Secretary determines that appropriate corrective action has been taken.

(2) DISCRETIONARY TERMINATION.—If a health information service violates a requirement or standard under this part and a penalty has been imposed under section 5110, the Secretary shall review the certification of the service and may terminate the certification.

SEC. 5108. HEALTH INFORMATION CONTINUITY

(a) INFORMATION HELD BY PLANS AND PROVIDERS.—If a health information plan sponsor or health service provider ceases to function, in a manner that would threaten the continued availability of the standard health information held by the sponsor or provider, the health information may be obtained by the State in which the sponsor or provider is located.

(b) INFORMATION HELD BY HEALTH INFORMATION NETWORK SERVICES.—If a health information network service is decertified or ceases to function, in a manner that would threaten the continued availability of the standard health information held by the service, the health information shall be transferred to a health information network service that is certified under section 5106 and designated by the Secretary to receive the information.

SEC. 5109. IMPOSITION OF ADDITIONAL REQUIREMENTS.

(a) IN GENERAL.—After the Secretary establishes standards under section 5103 that are necessary to make a set of health information described in section 5103(b) comparable and compatible for electronic transmission, a health information plan sponsor or a health service provider may not require health information plan sponsor or health service provider to provide in any manner any health information that is not included in such set in connection with a transaction described in subsection (a)(2) or (b)(2) of section 5104 unless—

(1) the sponsor or provider voluntarily agrees to the imposition of such additional requirement; or

(2) a waiver is granted under subsection (b) to establish such additional requirement.

(b) CONDITIONS FOR WAIVERS.—

(1) IN GENERAL.—A health information plan sponsor or health service provider may request a waiver from the Secretary in order to require a health information plan sponsor or health service provider to provide additional data described in subsection (a).

(2) CONSIDERATION OF WAIVER REQUESTS.—A waiver may not be granted under this subsection unless the Secretary determines that the value of the additional data to be provided for research or other purposes significantly outweighs the administrative cost of the im-

position of the additional requirement, taking into account the burden of the timing of the imposition of the additional requirement.

(3) ANONYMOUS REPORTING.—If a health information plan sponsor or a health service provider attempts to require a health information plan sponsor or health service provider to provide additional data described in subsection (a), the sponsor or provider on which such additional requirement is being imposed may contact the Secretary. The Secretary shall develop a procedure under which a sponsor or provider that contacts the Secretary under the preceding sentence shall remain anonymous. The Secretary shall notify the sponsor or provider imposing the additional requirement that the requirement may not be imposed unless the other sponsor or provider voluntarily agrees to such requirement or a waiver is obtained under this subsection.

SEC. 5110. CIVIL MONEY PENALTIES.

(a) IN GENERAL.—Any person who the Secretary determines is required, but has failed, to comply with a requirement or standard imposed under this part shall be subject, in addition to any other penalties that may be prescribed by law, to a civil money penalty of not more than $1,000 for each such failure.

(b) LIMITATIONS.—

(1) FAILURES DUE TO REASONABLE CAUSE.—

(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C) and paragraph (3), a penalty may not be imposed under subsection (a) if the failure to comply—

(i) was due to reasonable cause and not to willful neglect (including a failure by a person who did not know, and by exercising reasonable diligence would not have known, that the person failed to comply); and

(ii) is corrected during the 30-day period beginning on the 1st date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

(B) EXTENSION OF PERIOD.—The period referred to in subparagraph (A)(ii) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure involved.

(C) ASSISTANCE.—If the Secretary determines that a health information plan sponsor or health service provider failed to comply with a requirement or standard imposed under this part because the sponsor or provider was unable to comply, a penalty may not be imposed under subsection (a) and the Secretary may provide technical assistance to the sponsor or provider in any manner determined appropriate by the Secretary.

(2) WAIVER.—Except as provided in paragraph (3), in the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) that is not entirely waived under paragraph (1) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

(3) EXCEPTION.—Paragraphs (1) and (2) do not apply to a failure by a health information network service to comply with section 5108(b).

(c) ADMINISTRATIVE REVIEW.—

(1) OPPORTUNITY FOR HEARING.—A person assessed under subsection (a) shall be afforded an opportunity for hearing by the Secretary upon request made within 30 days after the date of the issuance of a notice of assessment. All hearings shall be determined on the record pursuant to section 554 of title 5, United States Code. If no hearing is requested, the assessment shall constitute a final and unappealable order.

(2) HEARING PROCEDURE.—If a hearing is requested, the initial agency decision shall be made by an administrative law judge, and such decision shall become the final order unless the Secretary modifies or vacates the decision. Notice of intent to modify or vacate the decision of the administrative law judge shall be issued to the parties within 30 days after the date of the decision of the judge. A final order which takes effect under this paragraph shall be subject to review only as provided under subsection (d).

(d) JUDICIAL REVIEW.—

(1) FILING OF ACTION FOR REVIEW.—Any person against whom an order imposing a civil money penalty has been entered after an agency hearing under this section may obtain review by the United States district court for any district in which such person is located or the United States District Court for the District of Columbia by filing a notice of appeal in such court within 30 days from the date of such order, and simultaneously sending a copy of such notice be registered mail to the Secretary.

(2) CERTIFICATION OF ADMINISTRATIVE RECORD.—The Secretary shall promptly certify and file in such court the record upon which the penalty was imposed.

(3) STANDARD FOR REVIEW.—The findings of the Secretary shall be set aside only if found to be unsupported by substantial evidence as provided by section 706(2)(E) of title 5, United States Code.

(4) APPEAL.—Any final decision, order, or judgment of such district court concerning such review shall be subject to appeal as provided in chapter 83 of title 28 of such Code.

(e) FAILURE TO PAY ASSESSMENT; MAINTENANCE OF ACTION.—

(1) FAILURE TO PAY ASSESSMENT.—If any person fails to pay an assessment after it has become a final and unappealable order, or after the court has entered final judgment in favor of the Secretary, the Secretary shall refer the matter to the Attorney General who shall recover the amount assessed by action in the appropriate United States district court.

(2) NONREVIEWABILITY.—In such action the validity and appropriateness of the final order imposing the penalty shall not be subject to review.

(f) PAYMENT OF PENALTIES.—Except as otherwise provided, penalties collected under this section shall be paid to the Secretary (or other officer) imposing the penalty and shall be available without appropriation and until expended for the purpose of enforcing the provisions with respect to which the penalty was imposed.

Subpart B—Miscellaneous Provisions

SEC. 5111. GENERAL REQUIREMENT ON SECRETARY.

In complying with any requirements imposed under this part, the Secretary shall rely on recommendations of the Health Information Advisory Committee established under section 5112 and shall consult with appropriate Federal agencies.

SEC. 5112. HEALTH INFORMATION ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—There is established a committee to be known as the Health Care Information Advisory Committee.

(b) DUTY.—The committee shall provide assistance to the Secretary in complying with the requirements imposed on the Secretary under this part. In performing such duty, the committee shall receive technical assistance from appropriate Federal agencies.

(c) MEMBERSHIP.—

(1) IN GENERAL.—The committee shall consist of 15 members to be appointed by the President not later than 60 days after the date of the enactment of this Act. The committee shall designate 1 member as the chairperson of the committee.

(2) EXPERTISE.—The membership of the committee shall consist of individuals who are of recognized standing and distinction and who possess the demonstrated capacity to discharge the duties imposed on the committee.

(3) TERMS.—Each member of the committee shall be appointed for a term of 5 years, except that the members first appointed shall serve staggered terms such that the terms of no more than 3 members expire at one time.

(4) VACANCIES.—

(A) IN GENERAL.—A vacancy on the committee shall be filled in the manner in which the original

appointment was made and shall be subject to any conditions which applied with respect to the original appointment.

(B) FILLING UNEXPIRED TERM.—An individual chosen to fill a vacancy shall be appointed for the unexpired term of the member replaced.

(C) EXPIRATION OF TERMS.—The term of any member shall not expire before the date on which the member's successor takes office.

(D) CONFLICTS OF INTEREST.—Members of the committee shall disclose upon appointment to the committee or at any subsequent time that it may occur, conflicts of interest.

(d) MEETINGS.—

(1) IN GENERAL.—Except as provided in paragraph (2), the committee shall meet at the call of the chairperson.

(2) INITIAL MEETING.—Not later than 30 days after the date on which all members of the committee have been appointed, the committee shall hold its first meeting.

(3) QUORUM.—A majority of the members of the committee shall constitute a quorum, but a lesser number of members may hold hearings.

(e) POWER TO HOLD HEARINGS.—The committee may hold such hearings, sit and act at such times and places, take such testimony, and receive such evidence as the committee considers advisable to carry out the purposes of this section.

(f) OTHER ADMINISTRATIVE PROVISIONS.—

(1) IN GENERAL.—The Panel may—

(A) employ and fix the compensation of an executive director and such other personnel (not to exceed 25) as may be necessary to carry out its duties (without regard to the provisions of title 5, United States Code, governing appointments in the competitive service);

(B) seek such assistance and support as may be required in the performance of its duties from appropriate Federal departments and agencies;

(C) enter into contracts or make other arrangements, as may be necessary for the conduct of the work of the Panel (without regard to section 3709 of the Revised Statues (41 U.S.C. 5));

(D) make advance, progress, and other payments which relate to the work of the Panel;

(E) provide transportation and subsistence for persons serving without compensation; and

(F) prescribe such rules and regulations as it deems necessary with respect to the internal organization and operation of the Panel.

(2) COMPENSATION.—While serving on the business of the Panel (including traveltime), a member of the Panel shall be entitled to compensation at the per

diem equivalent of the rate provided for level IV of the Executive Schedule under section 5315 of title 5, United States Code. While so serving away from home and the regular place of business of a member of the Panel, the member may be allowed travel expenses, as authorized by the chairperson of the Panel. Physicians serving as personnel of the Panel may be provided a physician comparability allowance by the Panel in the same manner as Government physicians may be provided such an allowance by an agency under section 5948 of title 5, United States Code, and for such purpose subsection (i) of such section shall apply to the Panel in the same manner as the subsection applies to the Tennessee Valley Authority. For purposes of pay (other than pay of members of the Panel) and employment benefits, rights, and privileges, all personnel of the Panel shall be treated as if they were employees of the United States Senate.

(3) GAO AUDITS.—The Panel shall be subject to periodic audit by the General Accounting Office.

(g) REPORTS.—

(1) IN GENERAL.—The committee shall annually prepare and submit to the Congress and the Secretary a report on—

(A) the status of the health information network established pursuant to this part, including—

(i) whether the network is fulfilling the purpose described in section 5101; and

(ii) information relating to the cost and quality of health care rendered by health service providers;

(B) the savings and costs of the network; and

(C) any legislative recommendations related to the network.

(2) AVAILABILITY TO THE PUBLIC.—Any information in the report submitted to the Congress under paragraph (1) shall be made available to the public unless such information may not be disclosed by law.

(h) DURATION.—Notwithstanding section 14(a) of the Federal Advisory Committee Act, the committee shall continue in existence under otherwise provided by law.

SEC. 5113. AUTHORITY TO MAKE GRANTS FOR DEMONSTRATION PROJECTS.

(a) IN GENERAL.—The Secretary may make grants for demonstration projects to promote the development and use of electronically integrated community-based health information systems and computerized patient medical records.

(b) APPLICATIONS.—

(1) SUBMISSION.—To apply for a grant under this section for any fiscal year, an applicant shall submit an application to the Secretary in accordance with the procedures established by the Secretary.

(2) CRITERIA FOR APPROVAL.—The Secretary may not approve an application submitted under paragraph (1) unless the application includes assurances satisfactory to the Secretary regarding the following:

(A) USE OF EXISTING TECHNOLOGY.—Funds received under this section will be used to apply telecommunications and information systems technology that is in existence on the date the application is submitted in a manner that improves the quality of health care, reduces the costs of such care, and protects the privacy and confidentiality of information relating to the physical or mental condition of an individual.

(B) USE OF EXISTING INFORMATION SYSTEMS.—Funds received under this section will be used—

(i) to enhance telecommunications or information systems that are operating on the date the application is submitted;

(ii) to integrate telecommunications or information systems that are operating on the date the application is submitted; or

(iii) to connect additional users to telecommunications or information networks or systems that are operating on the date the application is submitted.

(C) MATCHING FUNDS.—The applicant will make available funds for the demonstration project in an amount that equals at least 50 percent of the cost of the project.

(c) GEOGRAPHIC DIVERSITY.—In making any grants under this section, the Secretary shall make grants to persons representing different geographic areas of the United States, including urban and rural areas.

(d) REVIEW AND SANCTIONS.—The Secretary shall review at least annually the compliance of a person receiving a grant under this section with the provisions of this section. The Secretary shall establish a procedure for determining whether such a person has failed to comply substantially within the provisions of this section and the sanctions to be imposed for any such noncompliance.

(e) ANNUAL REPORT.—The Secretary shall transmit annually to the President and the Congress a report containing a detailed statement of the activities carried out under this section in the preceding 12 months.

SEC. 5114. EFFECT ON STATE LAW.

(a) IN GENERAL.—A provision, requirement, or standard under this part shall supersede a provision of State law that requires medical or health records (including billing information) to be maintained in written rather than electronic form, except where the Secretary determines that the provision is necessary to prevent fraud and abuse, with respect to controlled substances, or for other purposes.

(b) PUBLIC HEALTH REPORTING.—Nothing in this part shall be construed to invalidate or limit the authority,

power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

Page 882, beginning on line 19, strike "National Health Board" and insert "Secretary".

Page 882, line 20, strike "modify, update, or".

Page 882, strike line 23 and insert "a standard under part 1 that is inconsistent with the form or requirement.".

Beginning on page 885, strike line 11 through page 886, line 3 (and redesignate provisions accordingly).

Amend part 2 of subtitle B of title V (pages 871 through 877) to read as follows (and redesignate provisions and conform the table of contents of title V accordingly):

PART 2—FAIR HEALTH INFORMATION PRACTICES

SEC. 5120. DEFINITIONS.

(a) DEFINITIONS RELATING TO PROTECTED HEALTH INFORMATION.—For purposes of this part:

(1) DISCLOSE.—The term "disclose", when used with respect to protected health information that is held by a health information trustee, means to provide access to the information, but only if such access is provided by the trustee to a person other than—

(A) the trustee or an officer or employee of the trustee;

(B) an affiliated person of the trustee; or

(C) a protected individual who is a subject of the information.

(2) DISCLOSURE.—The term "disclosure" means the act or an instance of disclosing.

(3) PROTECTED HEALTH INFORMATION.—The term "protected health information" means any information, whether oral or recorded in any form or medium—

(A) that is created or received in a State by—

(i) a health care provider;

(ii) a health benefit plan sponsor;

(iii) a health oversight agency;

(iv) a health information service organization; or

(v) a public health authority;

(B) that relates in any way to the past, present, or future physical or mental health or condition or functional status of a protected individual, the provision of health care to a protected individual,

or payment for the provision of health care to a protected individual; and

(C) that—

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(4) PROTECTED INDIVIDUAL.—The term "protected individual" means an individual who, with respect to a date—

(A) is living on the date; or

(B) has died within the 2-year period ending on the date.

(5) USE.—The term "use", when used with respect to protected health information that is held by a health information trustee, means—

(A) to use, or provide access to, the information in any manner that does not constitute a disclosure; or

(B) any act or instance of using, or providing access, described in subparagraph (A).

(b) DEFINITIONS RELATING TO HEALTH INFORMATION TRUSTEES.—For purposes of this part:

(1) CARRIER.—The term "carrier" means a licensed insurance company, a hospital or medical service corporation (including an existing Blue Cross or Blue Shield organization, within the meaning of section 833(c)(2) of the Internal Revenue Code of 1986), a health maintenance organization, or other entity licensed or certified by a State to provide health insurance or health benefits.

(2) HEALTH BENEFIT PLAN.—The term "health benefit plan" means—

(A) any contract of health insurance, including any hospital or medical service policy or certificate, hospital or medical service plan contract, or health maintenance organization group contract, that is provided by a carrier; and

(B) an employee welfare benefit plan or other arrangement insofar as the plan or arrangement provides health benefits and is funded in a manner other than through the purchase of one or more policies or contracts described in subparagraph (A).

(3) HEALTH BENEFIT PLAN SPONSOR.—The term "health benefit plan sponsor" means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a carrier providing a regional alliance health plan;

(B) an eligible sponsor (as defined in section 1311(b)) providing a corporate alliance health plan;

(C) a carrier or other person providing any other health benefit plan, including any public entity that provides payments for health care items and services under a health benefit plan that are equivalent to payments provided by a private person under such a plan; or

(D) an officer or employee of a person described in subparagraph (A), (B), or (C).

(4) HEALTH CARE PROVIDER.—The term "health care provider" means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a person who is licensed, certified, registered, or otherwise authorized by law to provide an item or service that constitutes health care in the ordinary course of business or practice of a profession;

(B) a Federal or State program that directly provides items or services that constitute health care to beneficiaries; or

(C) an officer or employee of a person described in subparagraph (A) or (B).

(5) HEALTH INFORMATION SERVICE ORGANIZATION.—The term "health information service organization" means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a person, other than an affiliated person, who performs specific functions for which the Secretary has authorized (by means of a designation or certification) the person to receive access to health care data in electronic or magnetic form that are regulated by this Act; or

(B) an officer or employee of a person described in subparagraph (A).

(6) HEALTH INFORMATION TRUSTEE.—The term "health information trustee" means—

(A) a health care provider;

(B) a health information service organization;

(C) a health oversight agency;

(D) a health benefit plan sponsor;

(E) a public health authority;

(F) a health researcher;

(G) a person who, with respect to a specific item of protected health information, is not described in subparagraphs (A) through (F) but receives the information—

(i) pursuant to—

(I) section 5137 (relating to emergency circumstances);

(II) section 5138 (relating to judicial and administrative purposes);

(III) section 5139 (relating to law enforcement); or

(IV) section 5140 (relating to subpoenas, warrants, and search warrants); or

(ii) while acting in whole or in part in the capacity of an officer or employee of a person described in clause (i).

(7) HEALTH OVERSIGHT AGENCY.—The term "health oversight agency" means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) a person who performs or oversees the performance of an assessment, evaluation, determination, or investigation relating to the licensing, accreditation, or certification of health care providers;

(B) a person who—

(i) performs or oversees the performance of an audit, assessment, evaluation, determination, or investigation relating to the effectiveness of, compliance with, or applicability of, legal, fiscal, medical, or scientific standards or aspects of performance related to the delivery of, or payment for, health care; and

(ii) is a public agency, acting on behalf of a public agency, acting pursuant to a requirement of a public agency, or carrying out activities under a State or Federal statute regulating the assessment, evaluation, determination, or investigation; or

(C) an officer or employee of a person described in subparagraph (A) or (B).

(8) HEALTH RESEARCHER.—The term "health researcher" means a person who, with respect to a specific item of protected health information, receives the information—

(A) pursuant to section 5136 (relating to health research); or

(B) while acting in whole or in part in the capacity of an officer or employee of a person described in subparagraph (A).

(9) PUBLIC HEALTH AUTHORITY.—The term "public health authority" means a person who, with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

(A) an authority of the United States, a State, or a political subdivision of a State that is responsible for public health matters;

(B) a person acting under the direction of such an authority; or

(C) an officer or employee of a person described in subparagraph (A) or (B).

(c) OTHER DEFINITIONS.—For purposes of this part:

(1) AFFILIATED PERSON.—The term "affiliated person" means a person who—

(A) is not a health information trustee;

(B) is a contractor, subcontractor, associate, or subsidiary of a person who is a health information trustee; and

(C) pursuant to an agreement or other relationship with such trustee, receives, creates, uses, maintains, or discloses protected health information.

(2) APPROVED HEALTH RESEARCH PROJECT.—The term "approved health research project" means a biomedical, epidemiological, or health services research or statistics project, or a research project on behavioral and social factors affecting health, that has been approved by a certified institutional review board.

(3) CERTIFIED INSTITUTIONAL REVIEW BOARD.—The term "certified institutional review board" means a board—

(A) established by an entity to review research involving protected health information and the rights of protected individuals conducted at or supported by the entity;

(B) established in accordance with regulations of the Secretary under section 5136(d)(1); and

(C) certified by the Secretary under section 5136(d)(2).

(4) HEALTH CARE.—The term "health care"—

(A) means—

(i) any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure—

(I) with respect to the physical or mental condition, or functional status, of an individual; or

(II) affecting the structure or function of the human body or any part of the human body, including banking of blood, sperm, organs, or any other tissue; or

(ii) any sale or dispensing of a drug, device, equipment, or other item to an individual, or for the use of an individual, pursuant to a prescription; but

(B) does not include any item or service that is not furnished for the purpose of maintaining or improving the health of an individual.

(5) LAW ENFORCEMENT INQUIRY.—The term "law enforcement inquiry" means a lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant to such a statute.

(6) PERSON.—The term "person" includes an authority of the United States, a State, or a political subdivision of a State.

Subpart A—Duties of Health Information Trustees

SEC. 5121. INSPECTION OF PROTECTED HEALTH INFORMATION.

(a) IN GENERAL.—Except as provided in subsection (b), a health information trustee described in subsection (g)—

(1) shall permit a protected individual to inspect any protected health information about the individual that the trustee maintains, any accounting with respect to such information required under section 5124, and any copy of an authorization required under section 5132 that pertains to such information;

(2) shall provide the protected individual with a copy of the information upon request by the individual and subject to any conditions imposed by the trustee under subsection (d);

(3) shall permit a person who has been designated in writing by the protected individual to inspect the information on behalf of the individual or to accompany the individual during the inspection; and

(4) may offer to explain or interpret information that is inspected or copied under this subsection.

(b) EXCEPTIONS.—A health information trustee is not required by this section to permit inspection or copying of protected health information by a protected individual if any of the following conditions apply:

(1) MENTAL HEALTH TREATMENT NOTES.—The information consists of psychiatric, psychological, or mental health treatment notes about the individual, the trustee determines in the exercise of reasonable professional judgment that inspection or copying of the notes would cause sufficient harm to the protected individual so as to outweigh the desirability of permitting access, and the trustee does not disclose the notes to any person not directly engaged in treating the individual, except with the authorization of the individual or under compulsion of law.

(2) INFORMATION ABOUT OTHERS.—The information relates to an individual, other than the protected individual or a health care provider, and the trustee determines in the exercise of reasonable professional judgment that inspection or copying of the information would cause sufficient harm to one or both of the indi-

viduals so as to outweigh the desirability of permitting access.

(3) ENDANGERMENT TO LIFE OR SAFETY.—Inspection or copying of the information could reasonably be expected to endanger the life or physical safety of an individual.

(4) CONFIDENTIAL SOURCE.—The information identifies or could reasonably lead to the identification of an individual (other than a health care provider) who provided information under a promise of confidentiality to a health care provider concerning a protected individual who is a subject of the information.

(5) ADMINISTRATIVE PURPOSES.—The information—

(A) is used by the trustee solely for administrative purposes and not in the provision of health care to a protected individual who is a subject of the information; and

(B) is not disclosed by the trustee to any person.

(6) DUPLICATIVE INFORMATION.—The information duplicates information available for inspection under subsection (a).

(7) INFORMATION COMPILED IN ANTICIPATION OF LITIGATION.—The information is compiled principally—

(A) in anticipation of a civil, criminal, or administrative action or proceeding; or

(B) for use in such an action or proceeding.

(c) INSPECTION AND COPYING OF SEGREGABLE PORTION.—A health information trustee shall permit inspection and copying under subsection (a) of any reasonably segregable portion of a record after deletion of any portion that is exempt under subsection (b).

(d) CONDITIONS.—A health information trustee may—

(1) require a written request for the inspection and copying of protected health information under this section; and

(2) charge a reasonable cost-based fee for—

(A) permitting inspection of information under this section; and

(B) providing a copy of protected health information under this section.

(e) STATEMENT OF REASONS FOR DENIAL.—If a health information trustee denies in whole or in part a request for inspection or copying under this section, the trustee shall provide the protected individual who made the request with a written statement of the reasons for the denial.

(f) DEADLINE.—A health information trustee shall comply with or deny a request for inspection or copying of protected health information under this section within the 30-day period beginning on the date the trustee receives the request.

(g) APPLICABILITY.—This section applies to a health information trustee who is—

(1) a health benefit plan sponsor;

(2) a health care provider;

(3) a health information service organization;
(4) a health oversight agency; or
(5) a public health authority.

SEC. 5122. AMENDMENT OF PROTECTED HEALTH INFORMATION.

(a) IN GENERAL.—A health information trustee described in subsection (f) shall, within the 45-day period beginning on the date the trustee receives from a protected individual about whom the trustee maintains protected health information a written request that the trustee correct or amend the information, complete the duties described in one of the following paragraphs:

(1) CORRECTION OR AMENDMENT AND NOTIFICATION.—The trustee shall—

(A) make the correction or amendment requested;

(B) inform the protected individual of the amendment or correction that has been made;

(C) make reasonable efforts to inform any person who is identified by the protected individual, who is not an employee of the trustee, and to whom the uncorrected or unamended portion of the information was previously disclosed of the correction or amendment that has been made; and

(D) at the request of the individual, make reasonable efforts to inform any known source of the uncorrected or unamended portion of the information about the correction or amendment that has been made.

(2) REASONS FOR REFUSAL AND REVIEW PROCEDURES.—The trustee shall inform the protected individual of—

(A) the reasons for the refusal of the trustee to make the correction or amendment;

(B) any procedures for further review of the refusal; and

(C) the individual's right to file with the trustee a concise statement setting forth the requested correction or amendment and the individual's reasons for disagreeing with the refusal of the trustee.

(b) STANDARDS FOR CORRECTION OR AMENDMENT.—A trustee shall correct or amend protected health information in accordance with a request made under subsection (a) if the trustee determines that the information is not accurate, relevant, timely, or complete for the purposes for which the information may be used or disclosed by the trustee.

(c) STATEMENT OF DISAGREEMENT.—After a protected individual has filed a statement of disagreement under subsection (a)(2)(C), the trustee, in any subsequent disclosure of the disputed portion of the information, shall include a copy of the individual's statement and may include a con-

cise statement of the trustee's reasons for not making the requested correction or amendment.

(d) CONSTRUCTION.—This section may not be construed to require a health information trustee to conduct a hearing or proceeding concerning a request for a correction or amendment to protected health information the trustee maintains.

(e) CORRECTION.—For purposes of subsection (a), a correction is deemed to have been made to protected health information when—

(1) information that is not timely, accurate, relevant, or complete is clearly marked as incorrect; or

(2) supplementary correct information is made part of the information and adequately cross-referenced.

(f) APPLICABILITY.—This section applies to a health information trustee who is—

(1) a health benefit plan sponsor;

(2) a health care provider;

(3) a health information service organization;

(4) a health oversight agency; or

(5) a public health authority.

SEC. 5123. NOTICE OF INFORMATION PRACTICES.

(a) PREPARATION OF NOTICE.—A health information trustee described in subsection (d) shall prepare a written notice of information practices describing the following:

(1) The rights under this part of a protected individual who is the subject of protected health information, including the right to inspect and copy such information and the right to seek amendments to such information, and the procedures for authorizing disclosures of protected health information and for revoking such authorizations.

(2) The procedures established by the trustee for the exercise of such rights.

(3) The uses and disclosures of protected health information that are authorized under this part.

(b) DISSEMINATION OF NOTICE.—A health information trustee—

(1) shall, upon request, provide any person with a copy of the trustee's notice of information practices (described in subsection (a)); and

(2) shall make reasonable efforts to inform persons in a clear and conspicuous manner of the existence and availability of such notice.

(c) MODEL NOTICES.—Not later than July 1, 1996, the Secretary, after notice and opportunity for public comment, shall develop and disseminate model notices of information practices for use by health information trustees under this section.

(d) APPLICABILITY.—This section applies to a health information trustee who is—

(1) a health benefit plan sponsor;

(2) a health care provider;

(3) a health information service organization; or

(4) a health oversight agency.

SEC. 5124. ACCOUNTING FOR DISCLOSURES.

(a) IN GENERAL.—Except as provided in subsection (b) and section 5134, each health information trustee shall create and maintain, with respect to any protected health information the trustee discloses, a record of—

(1) the date and purpose of the disclosure;

(2) the name of the person to whom the disclosure was made;

(3) the address of the person to whom the disclosure was made or the location to which the disclosure was made; and

(4) where practicable, a description of the information disclosed.

(b) REGULATIONS.—Not later than July 1, 1996, the Secretary shall promulgate regulations that exempt a health information trustee from maintaining a record under subsection (a) with respect protected health information disclosed by the trustee for purposes of peer review, licensing, certification, accreditation, and similar activities.

SEC. 5125. SECURITY.

(a) IN GENERAL.—Each health information trustee who receives or creates protected health information that is subject to this part shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

(1) to ensure the integrity and confidentiality of the information;

(2) to protect against any reasonably anticipated—

(A) threats or hazards to the security or integrity of the information; and

(B) unauthorized uses or disclosures of the information; and

(3) otherwise ensure compliance with this part by the trustee and the officers and employees of the trustee.

(b) GUIDELINES.—Not later than July 1, 1996, the Secretary, after notice and opportunity for public comment, shall develop and disseminate guidelines for the implementation of this section. The guidelines shall take into account—

(1) the technical capabilities of record systems used to maintain protected health information;

(2) the costs of security measures;

(3) the need for training persons who have access to protected health information; and

(4) the value of audit trails in computerized record systems.

Subpart B—Use and Disclosure of Protected Health Information

SEC. 5131. GENERAL LIMITATIONS ON USE AND DISCLOSURE.

(a) USE.—Except as otherwise provided under this part, a health information trustee may use protected health information only for a purpose—

(1) that is compatible with and directly related to the purpose for which the information—

(A) was collected; or

(B) was received by the trustee; or

(2) for which the trustee is authorized to disclose the information under this part.

(b) DISCLOSURE.—A health information trustee may disclose protected health information only as authorized under this part.

(c) SCOPE OF USES AND DISCLOSURES.—

(1) IN GENERAL.—A use or disclosure of protected health information by a health information trustee shall be limited, when practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed.

(2) GUIDELINES.—Not later than July 1, 1996, the Secretary, after notice and opportunity for public comment, shall issue guidelines to implement paragraph (1), which shall take into account the technical capabilities of the record systems used to maintain protected health information and the costs of limiting use and disclosure.

(d) IDENTIFICATION OF DISCLOSED INFORMATION AS PROTECTED INFORMATION.—Except with respect to protected health information that is disclosed under section 5134 (relating to next of kin and directory information), a health information trustee may disclose protected health information only if the recipient has been notified that the information is protected health information that is subject to this part.

(e) AGREEMENT TO LIMIT USE OR DISCLOSURE.—A health information trustee who receives protected health information from any person pursuant to a written agreement to restrict use or disclosure of the information to a greater extent than otherwise would be required under this part shall comply with the terms of the agreement, except where use or disclosure of the information in violation of the agreement is required by law. A trustee who fails to comply with the preceding sentence shall be subject to section 5171 (relating to civil actions) with respect to such failure.

(f) NO GENERAL REQUIREMENT TO DISCLOSE.—Nothing in this part shall be construed to require a health information trustee to disclose protected health information not otherwise required to be disclosed by law.

SEC. 5132. AUTHORIZATIONS FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION.

(a) WRITTEN AUTHORIZATIONS.—A health information trustee, other than a health information service organization, may disclose protected health information pursuant to an authorization executed by the protected individual who is the subject of the information, if each of the following requirements is satisfied:

(1) WRITING.—The authorization is in writing, signed by the individual, and dated on the date of such signature.

(2) SEPARATE FORM.—The authorization is not on a form used to authorize or facilitate the provision of, or payment for, health care.

(3) TRUSTEE DESCRIBED.—The trustee is specifically named or generically described in the authorization as authorized to disclose such information.

(4) RECIPIENT DESCRIBED.—The person to whom the information is to be disclosed is specifically named or generically described in the authorization as a person to whom such information may be disclosed.

(5) STATEMENT OF INTENDED USES AND DISCLOSURES RECEIVED.—The authorization contains an acknowledgment that the individual has received a statement described in subsection (b) from such person.

(6) INFORMATION DESCRIBED.—The information to be disclosed is described in the authorization.

(7) AUTHORIZATION TIMELY RECEIVED.—The authorization is received by the trustee during a period described in subsection (c)(1).

(8) DISCLOSURE TIMELY MADE.—The disclosure occurs during a period described in subsection (c)(2).

(b) STATEMENT OF INTENDED USES AND DISCLOSURES.—

(1) IN GENERAL.—A person who wishes to receive from a health information trustee protected health information about a protected individual pursuant to an authorization executed by the individual shall supply the individual, in writing and on a form that is distinct from the authorization, with a statement of the uses for which the person intends the information and the disclosures the person intends to make of the information. Such statement shall be supplied before the authorization is executed.

(2) ENFORCEMENT.—If the person uses or discloses the information in a manner that is inconsistent with such statement, the person shall be subject to section 5171 (relating to civil actions) with respect to such failure, except where such use or disclosure is required by law.

(3) MODEL STATEMENTS.—Not later than July 1, 1996, the Secretary, after notice and opportunity for public comment, shall develop and disseminate model statements of intended uses and disclosures of the type described in paragraph (1).

(c) TIME LIMITATIONS ON AUTHORIZATIONS.—

(1) RECEIPT BY TRUSTEE.—For purposes of subsection (a)(7), an authorization is timely received if it is received by the trustee during—

(A) the 1-year period beginning on the date that the authorization is signed under subsection (a)(1), if the authorization permits the disclosure of protected health information to—

(i) a health benefit plan sponsor;

(ii) a health care provider;

(iii) a health oversight agency;

(iv) a public health authority;

(v) a health researcher; or

(vi) a person who provides counseling or social services to individuals; or

(B) the 30-day period beginning on the date that the authorization is signed under subsection (a)(1), if the authorization permits the disclosure of protected health information to a person other than a person described in subparagraph (A).

(2) DISCLOSURE BY TRUSTEE.—For purposes of subsection (a)(8), a disclosure is timely made if it occurs before—

(A) the date or event (if any) specified in the authorization upon which the authorization expires; and

(B) the expiration of the 6-month period beginning on the date the trustee receives the authorization.

(d) REVOCATION OR AMENDMENT OF AUTHORIZATION.—

(1) IN GENERAL.—A protected individual in writing may revoke or amend an authorization described in subsection (a), in whole or in part, at any time, except insofar as—

(A) disclosure of protected health information has been authorized to permit validation of expenditures based on health condition by a government authority; or

(B) action has been taken in reliance on the authorization.

(2) NOTICE OF REVOCATION.—A health information trustee who discloses protected health information in reliance on an authorization that has been revoked shall not be subject to any liability or penalty under this part if—

(A) the reliance was in good faith;

(B) the trustee had no notice of the revocation; and

(C) the disclosure was otherwise in accordance with the requirements of this section.

(e) ADDITIONAL REQUIREMENTS OF TRUSTEE.—A health information trustee may impose requirements for an authorization that are in addition to the requirements in this section.

(f) COPY.—A health information trustee who discloses protected health information pursuant to an authorization under this section shall maintain a copy of the authorization.

(g) CONSTRUCTION.—This section may not be construed—

(1) to require a health information trustee to disclose protected health information; or

(2) to limit the right of a health information trustee to charge a fee for the disclosure or reproduction of protected health information.

(h) SUBPOENAS, WARRANTS, AND SEARCH WARRANTS.—If a health information trustee discloses protected health information pursuant to an authorization in order to comply with an administrative subpoena or warrant or a judicial subpoena or search warrant, the authorization—

(1) shall specifically authorize the disclosure for the purpose of permitting the trustee to comply with the subpoena, warrant, or search warrant; and

(2) shall otherwise meet the requirements in this section.

SEC. 5133. TREATMENT, PAYMENT, AND OVERSIGHT.

(a) DISCLOSURES BY PLANS, PROVIDERS, AND OVERSIGHT AGENCIES.—A health information trustee described in subsection (d) may disclose protected health information to a health benefit plan sponsor, health care provider, or health oversight agency if the disclosure is—

(1) for the purpose of providing health care and a protected individual who is a subject of the information has not previously objected to the disclosure in writing;

(2) for the purpose of providing for the payment for health care furnished to an individual; or

(3) for use by a health oversight agency for a purpose that is described in subparagraph (A) or (B)(i) of section 5120(b)(7).

(b) DISCLOSURES BY CERTAIN OTHER TRUSTEES.—A health information trustee may disclose protected health information to a health care provider if—

(1) the disclosure is for the purpose described in subsection (a)(1); and

(2) the trustee—

(A) is a public health authority;

(B) received protected health information pursuant to section 5137 (relating to emergency circumstances); or

(C) is an officer or employee of a trustee described in subsection (B).

(c) USE IN ACTION AGAINST INDIVIDUAL.—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of

and related to receipt of health care or payment for health care.

(d) APPLICABILITY.—A health information trustee referred to in subsection (a) is any of the following:

(1) A health benefit plan sponsor.

(2) A health care provider.

(3) A health oversight agency.

(4) A health information service organization.

SEC. 5134. NEXT OF KIN AND DIRECTORY INFORMATION.

(a) NEXT OF KIN.—A health information trustee who is a health care provider, who received protected health information pursuant to section 5137 (relating to emergency circumstances), or who is an officer or employee of such a recipient may orally disclose protected health information about a protected individual to the next of kin of the individual (as defined under State law), or to a person with whom the individual has a close personal relationship, if—

(1) the trustee has no reason to believe that the individual would consider the information especially sensitive;

(2) the individual has not previously objected to the disclosure;

(3) the disclosure is consistent with good medical or other professional practice; and

(4) the information disclosed is limited to information about health care that is being provided to the individual at or about the time of the disclosure.

(b) DIRECTORY INFORMATION.—

(1) IN GENERAL.—A health information trustee who is a health care provider, who received protected health information pursuant to section 5137 (relating to emergency circumstances), or who is an officer or employee of such a recipient may disclose to any person the information described in paragraph (2) if—

(A) a protected individual who is a subject of the information has not objected in writing to the disclosure;

(B) the disclosure is otherwise consistent with good medical and other professional practice; and

(C) the information does not reveal specific information about the physical or mental condition or functional status of a protected individual or about the health care provided to a protected individual.

(2) INFORMATION DESCRIBED.—The information referred to in paragraph (1) is the following:

(A) The name of an individual receiving health care from a health care provider on a premises controlled by the provider.

(B) The location of the individual on such premises.

(C) The general health status of the individual, described in terms of critical, poor, fair, stable, satisfactory, or terms denoting similar conditions.

(c) NO ACCOUNTING REQUIRED.—A health information trustee who discloses protected health information under this section is not required to maintain an accounting of the disclosure under section 5124.

(d) RECIPIENTS.—A person to whom protected health information is disclosed under this section shall not, by reason of such disclosure, be subject to any requirement under this part.

SEC. 5135. PUBLIC HEALTH.

(a) IN GENERAL.—A health information trustee who is a health care provider or a public health authority may disclose protected health information to—

(1) a public health authority for use in legally authorized—

(A) disease or injury reporting;

(B) public health surveillance; or

(C) public health investigation or intervention; or

(2) an individual who is authorized by law to receive the information in a public health intervention.

(b) USE IN ACTION AGAINST INDIVIDUAL.—A public health authority who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except where the use or disclosure is authorized by law for protection of the public health.

(c) INDIVIDUAL RECIPIENTS.—An individual to whom protected health information is disclosed under subsection (a)(2) shall not, by reason of such disclosure, be subject to any requirement under this part.

SEC. 5136. HEALTH RESEARCH.

(a) IN GENERAL.—A health information trustee described in subsection (d) may disclose protected health information to a person if—

(1) the person is conducting an approved health research project;

(2) the information is to be used in the project; and

(3) the project has been determined by a certified institutional review board to be—

(A) of sufficient importance so as to outweigh the intrusion into the privacy of the protected individual who is the subject of the information that would result from the disclosure; and

(B) impracticable to conduct without the information.

(b) DISCLOSURES BY HEALTH INFORMATION SERVICE ORGANIZATIONS.—A health information service organization may disclose protected health information under subsection (a) only if the certified institutional review board referred to in subsection (a)(3) has been certified as being

qualified to make determinations under such subsection with respect to disclosures by such organizations.

(c) LIMITATIONS ON USE AND DISCLOSURE; OBLIGATIONS OF RECIPIENT.—A health researcher who receives protected health information about a protected individual pursuant to subsection (a)—

(1) may use the information solely for purposes of an approved health research project;

(2) may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual; and

(3) shall remove or destroy, at the earliest opportunity consistent with the purposes of the approved health research project in connection with which the disclosure was made, information that would enable an individual to be identified, unless a certified institutional review board has determined that there is a health or research justification for retention of such identifiers and there is an adequate plan to protect the identifiers from use and disclosure that is inconsistent with this part.

(d) APPLICABILITY.—A health information trustee referred to in subsection (a) is any health information trustee other than a person who, with respect to the specific protected health information to be disclosed under such subsection, received the information—

(1) pursuant to—

(A) section 5138 (relating to judicial and administrative purposes);

(B) paragraph (1), (2), or (3) of section 5139(a) (relating to law enforcement); or

(C) section 5140 (relating to subpoenas, warrants, and search warrants); or

(2) while acting in whole or in part in the capacity of an officer or employee of a person described in paragraph (1).

(e) REQUIREMENTS FOR INSTITUTIONAL REVIEW BOARDS.—

(1) REGULATIONS.—Not later than July 1, 1996, the Secretary, after opportunity for notice and comment, shall promulgate regulations establishing requirements for certified institutional review boards under this part. The regulations shall be based on regulations promulgated under section 491(a) of the Public Health Service Act and shall ensure that certified institutional review boards are qualified to assess and protect the confidentiality of research subjects. The regulations shall include specific requirements for certified institutional review boards that make determinations under subsection (a)(3) with respect to disclosures by health information service organizations.

(2) CERTIFICATION.—The Secretary shall certify that an institutional review board satisfies the require-

ments of the regulations promulgated under paragraph (1).

SEC. 5137. EMERGENCY CIRCUMSTANCES.

(a) IN GENERAL.—A health information trustee may disclose protected health information if the trustee believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual.

(b) USE IN ACTION AGAINST INDIVIDUAL.—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and related to receipt of health care or payment for health care.

SEC. 5138. JUDICIAL AND ADMINISTRATIVE PURPOSES.

(a) IN GENERAL.—A health information trustee described in subsection (d) may disclose protected health information—

(1) pursuant to the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, or comparable rules of other courts or administrative agencies in connection with litigation or proceedings to which a protected individual who is a subject of the information is a party and in which the individual has placed the individual's physical or mental condition or functional status in issue;

(2) if directed by a court in connection with a court-ordered examination of an individual; or

(3) to assist in the identification of a dead individual.

(b) WRITTEN STATEMENT.—A person seeking protected health information about a protected individual held by health information trustee under—

(1) subsection (a)(1)—

(A) shall notify the protected individual or the attorney of the protected individual of the request for the information;

(B) shall provide the trustee with a signed document attesting—

(i) that the protected individual is a party to the litigation or proceedings for which the information is sought;

(ii) that the individual has placed the individual's physical or mental condition or functional status in issue; and

(iii) the date on which the protected individual or the attorney of the protected individual was notified under subparagraph (A); and

(C) shall not accept any requested protected health information from the trustee until the ter-

mination of the 10-day period beginning on the date notice was given under subparagraph (A); or

(2) subsection (a)(3) shall provide the trustee with a written statement that the information is sought to assist in the identification of a dead individual.

(c) USE AND DISCLOSURE.—A person to whom protected health information is disclosed under this section may use and disclose the information only to accomplish the purpose for which the disclosure was made.

(d) APPLICABILITY.—A health information trustee referred to in subsection (a) is any of the following:

(1) A health benefit plan sponsor.

(2) A health care provider.

(3) A health oversight agency.

(4) A person who, with respect to the specific protected health information to be disclosed under such subsection, received the information—

(A) pursuant to—

(i) section 5137 (relating to emergency circumstances); or

(ii) section 5140 (relating to subpoenas, warrants, and search warrants); or

(B) while acting in whole or in part in the capacity of an officer or employee of a person described in subparagraph (A).

SEC. 5139. LAW ENFORCEMENT.

(a) IN GENERAL.—A health information trustee, other than a health information service organization, may disclose protected health information to a law enforcement agency, other than a health oversight agency—

(1) if the information is disclosed for use in an investigation or prosecution of a health information trustee;

(2) in connection with criminal activity committed against the trustee or an affiliated person of the trustee or on premises controlled by the trustee; or

(3) if the information is needed to determine whether a crime has been committed and the nature of any crime that may have been committed (other than a crime that may have been committed by the protected individual who is the subject of the information).

(b) ADDITIONAL AUTHORITY OF CERTAIN TRUSTEES.—A health information trustee who is not a health information service organization, a public health authority, or a health researcher may disclose protected health information to a law enforcement agency (other than a health oversight agency)—

(1) to assist in the identification or location of a victim, fugitive, or witness in a law enforcement inquiry;

(2) pursuant to a law requiring the reporting of specific health care information to law enforcement authorities; or

(3) if the information is specific health information described in paragraph (2) and the trustee is operated by a Federal agency;

(c) CERTIFICATION.—Where a law enforcement agency requests a health information trustee to disclose protected health information under subsection (a) or (b)(1), the agency shall provide the trustee with a written certification that—

(1) is signed by a supervisory official of a rank designated by the head of the agency;

(2) specifies the information requested; and

(3) states that the information is needed for a lawful purpose under this section.

(d) RESTRICTIONS ON DISCLOSURE AND USE.—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information—

(1) in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and directly related to the action or investigation for which the information was obtained; and

(2) otherwise unless the use or disclosure is necessary to fulfill the purpose for which the information was obtained and is not prohibited by any other provision of law.

SEC. 5140. SUBPOENAS, WARRANTS, AND SEARCH WARRANTS.

(a) IN GENERAL.—A health information trustee described in subsection (g) may disclose protected health information if the disclosure is pursuant to any of the following:

(1) A subpoena issued under the authority of a grand jury and the trustee is provided a written certification by the grand jury that the grand jury has complied with the applicable access provisions of section 5151.

(2) An administrative subpoena or warrant or a judicial subpoena or search warrant and the trustee is provided a written certification by the person seeking the information that the person has complied with the applicable access provisions of section 5151 or 5153(a).

(3) An administrative subpoena or warrant or a judicial subpoena or search warrant and the disclosure otherwise meets the conditions of one of sections 5133 through 5139.

(b) AUTHORITY OF ALL TRUSTEES.—Any health information trustee may disclose protected health information if the disclosure is pursuant to subsection (a)(3).

(c) RESTRICTIONS ON USE AND DISCLOSURE.—Protected health information about a protected individual that is disclosed by a health information trustee pursuant to—

(1) subsection (a)(2) may not be otherwise used or disclosed by the recipient unless the use or disclosure is necessary to fulfill the purpose for which the information was obtained; and

(2) subsection (a)(3) may not be used or disclosed by the recipient unless the recipient complies with the conditions and restrictions on use and disclosure with

which the recipient would have been required to comply if the disclosure by the trustee had been made under the section referred to in subsection (a)(3) the conditions of which were met by the disclosure.

(d) RESTRICTIONS ON GRAND JURIES.—Protected health information that is disclosed by a health information trustee under subsection (a)(1)—

(1) shall be returnable on a date when the grand jury is in session and actually presented to the grand jury;

(2) shall be used only for the purpose of considering whether to issue an indictment or report by that grand jury, or for the purpose of prosecuting a crime for which that indictment or report is issued, or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure or a comparable State rule;

(3) shall be destroyed or returned to the trustee if not used for one of the purposes specified in paragraph (2); and

(4) shall not be maintained, or a description of the contents of such information shall not be maintained, by any government authority other than in the sealed records of the grand jury, unless such information has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure or a comparable State rule.

(e) USE IN ACTION AGAINST INDIVIDUAL.—A person who receives protected health information about a protected individual through a disclosure under this section may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and directly related to the inquiry for which the information was obtained;

(f) CONSTRUCTION.—Nothing in this section shall be construed as authority for a health information trustee to refuse to comply with a valid administrative subpoena or warrant or a valid judicial subpoena or search warrant that meets the requirements of this part.

(g) APPLICABILITY.—A health information trustee referred to in subsection (a) is any trustee other than the following:

(1) A health information service organization.

(2) A public health authority.

(3) A health researcher.

SEC. 5141. HEALTH INFORMATION SERVICE ORGANIZATIONS.

A health information trustee may disclose protected health information to a health information service organization for the purpose of permitting the organization to perform a function for which the Secretary has authorized (by means of a designation or certification) the organization to receive access to health care data in electronic or magnetic form that are regulated by this Act .

Subpart C—Access Procedures and Challenge Rights

SEC. 5151. ACCESS PROCEDURES FOR LAW ENFORCEMENT SUBPOENAS, WARRANTS, AND SEARCH WARRANTS.

(a) PROBABLE CAUSE REQUIREMENT.—A government authority may not obtain protected health information about a protected individual from a health information trustee under paragraph (1) or (2) of section 5140(a) for use in a law enforcement inquiry unless there is probable cause to believe that the information is relevant to a legitimate law enforcement inquiry being conducted by the government authority.

(b) WARRANTS AND SEARCH WARRANTS.—A government authority that obtains protected health information about a protected individual from a health information trustee under circumstances described in subsection (a) and pursuant to a warrant or search warrant shall, not later than 30 days after the date the warrant was served on the trustee, serve the individual with, or mail to the last known address of the individual, a copy of the warrant.

(c) SUBPOENAS.—Except as provided in subsection (d), a government authority may not obtain protected health information about a protected individual from a health information trustee under circumstances described in subsection (a) and pursuant to a subpoena unless a copy of the subpoena has been served by hand delivery upon the individual, or mailed to the last known address of the individual, on or before the date on which the subpoena was served on the trustee, together with a notice (published by the Secretary under section 5155(1)) of the individual's right to challenge the subpoena in accordance with section 5152, and—

(1) 30 days have passed from the date of service, or 30 days have passed from the date of mailing, and within such time period the individual has not initiated a challenge in accordance with section 5152; or

(2) disclosure is ordered by a court under section 5152.

(d) APPLICATION FOR DELAY.—

(1) IN GENERAL.—A government authority may apply to an appropriate court to delay (for an initial period of not longer than 90 days) serving a copy of a subpoena and a notice otherwise required under subsection (c) with respect to a law enforcement inquiry. The government authority may apply to the court for extensions of the delay.

(2) REASONS FOR DELAY.—An application for a delay, or extension of a delay, under this subsection shall state, with reasonable specificity, the reasons why the delay or extension is being sought.

(3) EX PARTE ORDER.—The court shall enter an ex parte order delaying, or extending the delay of, the no-

tice and an order prohibiting the trustee from revealing the request for, or the disclosure of, the protected health information being sought if the court finds that—

(A) the inquiry being conducted is within the lawful jurisdiction of the government authority seeking the protected health information;

(B) there is probable cause to believe that the protected health information being sought is relevant to a legitimate law enforcement inquiry being conducted by the government authority;

(C) the government authority's need for the information outweighs the privacy interest of the protected individual who is the subject of the information; and

(D) there are reasonable grounds to believe that receipt of a notice by the individual will result in—

(i) endangering the life or physical safety of any individual;

(ii) flight from prosecution;

(iii) destruction of or tampering with evidence or the information being sought; or

(iv) intimidation of potential witnesses.

(4) SERVICE OF APPLICATION ON INDIVIDUAL.—Upon the expiration of a period of delay of notice under this subsection, the government authority shall serve upon the individual, with the service of the subpoena and the notice, a copy of any applications filed and approved under this subsection.

SEC. 5152. CHALLENGE PROCEDURES FOR LAW ENFORCEMENT SUBPOENAS.

(a) MOTION TO QUASH SUBPOENA.—Within 30 days of the date of service, or 30 days of the date of mailing, of a subpoena of a government authority seeking protected health information about a protected individual from a health information trustee under paragraph (1) or (2) of section 5140(a) (except a subpoena to which section 5153 applies), the individual may file (without filing fee) a motion to quash the subpoena—

(1) in the case of a State judicial subpoena, in the court which issued the subpoena;

(2) in the case of a subpoena issued under the authority of a State that is not a State judicial subpoena, in a court of competent jurisdiction;

(3) in the case of a subpoena issued under the authority of a Federal court, in any court of the United States of competent jurisdiction; or

(4) in the case of any other subpoena issued under the authority of the United States, in—

(A) the United States district court for the district in which the individual resides or in which the subpoena was issued; or

(B) another United States district court of competent jurisdiction.

(b) COPY.—A copy of the motion shall be served by the individual upon the government authority by delivery of registered or certified mail.

(c) AFFIDAVITS AND SWORN DOCUMENTS.—The government authority may file with the court such affidavits and other sworn documents as sustain the validity of the subpoena. The individual may file with the court, within 5 days of the date of the authority's filing, affidavits and sworn documents in response to the authority's filing. The court, upon the request of the individual, the government authority, or both, may proceed in camera.

(d) PROCEEDINGS AND DECISION ON MOTION.—The court may conduct such proceedings as it deems appropriate to rule on the motion. All such proceedings shall be completed, and the motion ruled on, within 10 calendar days of the date of the government authority's filing.

(e) EXTENSION OF TIME LIMITS FOR GOOD CAUSE.—The court, for good cause shown, may at any time in its discretion enlarge the time limits established by subsections (c) and (d).

(f) STANDARD FOR DECISION.—A court may deny a motion under subsection (a) if it finds that there is probable cause to believe that the protected health information being sought is relevant to a legitimate law enforcement inquiry being conducted by the government authority, unless the court finds that the individual's privacy interest outweighs the government authority's need for the information. The individual shall have the burden of demonstrating that the individual's privacy interest outweighs the need established by the government authority for the information.

(g) SPECIFIC CONSIDERATIONS WITH RESPECT TO PRIVACY INTEREST.—In determining under subsection (f) whether an individual's privacy interest outweighs the government authority's need for the information, the court shall consider—

(1) the particular purpose for which the information was collected by the trustee;

(2) the degree to which disclosure of the information will embarrass, injure, or invade the privacy of the individual;

(3) the effect of the disclosure on the individual's future health care;

(4) the importance of the inquiry being conducted by the government authority, and the importance of the information to that inquiry; and

(5) any other factor deemed relevant by the court.

(h) ATTORNEY'S FEES.—In the case of any motion brought under subsection (a) in which the individual has substantially prevailed, the court, in its discretion, may assess against a government authority a reasonable attor-

ney's fee and other litigation costs (including expert fees) reasonably incurred.

(i) NO INTERLOCUTORY APPEAL.—A court ruling denying a motion to quash under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the individual. An appeal of such a ruling may be taken by the individual within such period of time as is provided by law as part of any appeal from a final order in any legal proceeding initiated against the individual arising out of or based upon the protect health information disclosed.

SEC. 5153. ACCESS AND CHALLENGE PROCEDURES FOR OTHER SUBPOENAS.

(a) IN GENERAL.—A person (other than a government authority seeking protected health information under circumstances described in section 5151(a)) may not obtain protected health information about a protected individual from a health information trustee pursuant to a subpoena under section 5140(a)(2) unless—

(1) a copy of the subpoena has been served upon the individual or mailed to the last known address of the individual on or before the date on which the subpoena was served on the trustee, together with a notice (published by the Secretary under section 5155(2)) of the individual's right to challenge the subpoena, in accordance with subsection (b); and

(2) either—

(A) 30 days have passed from the date of service or 30 days have passed from the date of the mailing and within such time period the individual has not initiated a challenge in accordance with subsection (b); or

(B) disclosure is ordered by a court under such subsection.

(b) MOTION TO QUASH.—Within 30 days of the date of service or 30 days of the date of mailing of a subpoena seeking protected health information about a protected individual from a health information trustee under subsection (a), the individual may file (without filing fee) in any court of competent jurisdiction, a motion to quash the subpoena, with a copy served on the person seeking the information. The individual may oppose, or seek to limit, the subpoena on any grounds that would otherwise be available if the individual were in possession of the information.

(c) STANDARD FOR DECISION.—The court shall grant an individual's motion under subsection (b) if the person seeking the information has not sustained the burden of demonstrating that—

(1) there are reasonable grounds to believe that the information will be relevant to a lawsuit or other judicial or administrative proceeding; and

(2) the need of the person for the information outweighs the privacy interest of the individual.

(d) SPECIFIC CONSIDERATIONS WITH RESPECT TO PRIVACY INTEREST.—In determining under subsection (c) whether the need of the person for the information outweighs the privacy interest of the individual, the court shall consider—

(1) the particular purpose for which the information was collected by the trustee;

(2) the degree to which disclosure of the information will embarrass, injure, or invade the privacy of the individual;

(3) the effect of the disclosure on the individual's future health care;

(4) the importance of the information to the lawsuit or proceeding; and

(5) any other factor deemed relevant by the court.

(e) ATTORNEY'S FEES.—In the case of any motion brought under subsection (b) by an individual against a person in which the individual has substantially prevailed, the court, in its discretion, may assess against the person a reasonable attorney's fee and other litigation costs (including expert fees) reasonably incurred.

SEC. 5154. CONSTRUCTION OF SUBPART; SUSPENSION OF STATUTE OF LIMITATIONS.

(a) IN GENERAL.—Nothing in this subpart shall affect the right of a health information trustee to challenge a request for protected health information. Nothing in this subpart shall entitle a protected individual to assert the rights of a health information trustee.

(b) EFFECT OF MOTION ON STATUTE OF LIMITATIONS.—If an individual who is the subject of protected health information files a motion under this subpart which has the effect of delaying the access of a government authority to such information, the period beginning on the date such motion was filed and ending on the date on which the motion is decided shall be excluded in computing any period of limitations within which the government authority may commence any civil or criminal action in connection with which the access is sought.

SEC. 5155. RESPONSIBILITIES OF SECRETARY.

Not later than July 1, 1996, the Secretary, after notice and opportunity for public comment, shall develop and disseminate brief, clear, and easily understood model notices—

(1) for use under subsection (c) of section 5151, detailing the rights of a protected individual who wishes to challenge, under section 5152, the disclosure of protected health information about the individual under such subsection; and

(2) for use under subsection (a) of section 5153, detailing the rights of a protected individual who wishes to challenge, under subsection (b) of such section, the disclosure of protected health information about the individual under such section.

Subpart D—Miscellaneous Provisions

SEC. 5161. PAYMENT CARD AND ELECTRONIC PAYMENT TRANSACTIONS.

(a) PAYMENT FOR HEALTH CARE THROUGH CARD OR ELECTRONIC MEANS.—If a protected individual pays a health information trustee for health care by presenting a debit, credit, or other payment card or account number, or by any other electronic payment means, the trustee may disclose to a person described in subsection (b) only such protected health information about the individual as is necessary for the processing of the payment transaction or the billing or collection of amounts charged to, debited from, or otherwise paid by, the individual using the card, number, or other electronic payment means.

(b) TRANSACTION PROCESSING.—A person who is a debit, credit, or other payment card issuer, is otherwise directly involved in the processing of payment transactions involving such cards or other electronic payment transactions, or is otherwise directly involved in the billing or collection of amounts paid through such means, may only use or disclose protected health information about a protected individual that has been disclosed in accordance with subsection (a) when necessary for—

(1) the authorization, settlement, billing or collection of amounts charged to, debited from, or otherwise paid by, the individual using a debit, credit, or other payment card or account number, or by other electronic payment means;

(2) the transfer of receivables, accounts, or interest therein;

(3) the audit of the credit, debit, or other payment card account information;

(4) compliance with Federal, State, or local law; or

(5) a properly authorized civil, criminal, or regulatory investigation by Federal, State, or local authorities.

SEC. 5162. ACCESS TO PROTECTED HEALTH INFORMATION OUTSIDE OF THE UNITED STATES.

(a) IN GENERAL.—Notwithstanding the provisions of subpart B, and except as provided in subsection (b), a health information trustee may not permit any person who is not in a State to have access to protected health information about a protected individual unless one or more of the following conditions exist:

(1) SPECIFIC AUTHORIZATION.—The individual has specifically consented to the provision of such access outside of the United States in an authorization that meets the requirements of section 5132.

(2) EQUIVALENT PROTECTION.—The provision of such access is authorized under this part and the Secretary has determined that there are fair information practices for protected health information in the jurisdiction where the access will be provided that provide

protections for individuals and protected health information that are equivalent to the protections provided for by this part.

(3) ACCESS REQUIRED BY LAW.—The provision of such access is required under—

(A) a Federal statute; or

(B) a treaty or other international agreement applicable to the United States.

(b) EXCEPTIONS.—Subsection (a) does not apply where the provision of access to protected health information—

(1) is to a foreign public health authority;

(2) is authorized under section 5134 (relating to next of kin and directory information), 5136 (relating to health research), or 5137 (relating to emergency circumstances); or

(3) is necessary for the purpose of providing for payment for health care that has been provided to an individual.

SEC. 5163. STANDARDS FOR ELECTRONIC DOCUMENTS AND COMMUNICATIONS.

(a) STANDARDS.—Not later than July 1, 1996, the Secretary, after notice and opportunity for public comment and in consultation with appropriate private standard-setting organizations and other interested parties, shall establish standards with respect to the creation, transmission, receipt, and maintenance, in electronic and magnetic form, of each type of written document specifically required or authorized under this part. Where a signature is required under any other provision of this part, such standards shall provide for an electronic or magnetic substitute that serves the functional equivalent of a signature.

(b) TREATMENT OF COMPLYING DOCUMENTS AND COMMUNICATIONS.—An electronic or magnetic document or communication that satisfies the standards established under subsection (a) with respect to such document or communication shall be treated as satisfying the requirements of this part that apply to an equivalent written document.

SEC. 5164. DUTIES AND AUTHORITIES OF AFFILIATED PERSONS.

(a) REQUIREMENTS ON TRUSTEES.—

(1) PROVISION OF INFORMATION.—A health information trustee may provide protected health information to a person who, with respect to the trustee, is an affiliated person and may permit the affiliated person to use such information, only for the purpose of conducting, supporting, or facilitating an activity that the trustee is authorized to undertake.

(2) NOTICE TO AFFILIATED PERSON.—A health information trustee shall notify a person who, with respect to the trustee, is an affiliated person of any duties under this part that the affiliated person is required to fulfill and of any authorities under this part that the affiliated person is authorized to exercise.

(b) DUTIES OF AFFILIATED PERSONS.—

(1) IN GENERAL.—An affiliated person shall fulfill any duty under this part that—

(A) the health information trustee with whom the person has an agreement or relationship described in section 5120(c)(1)(C) is required to fulfill; and

(B) the person has undertaken to fulfill pursuant to such agreement or relationship.

(2) CONSTRUCTION OF OTHER SUBPARTS.—With respect to a duty described in paragraph (1) that an affiliated person is required to fulfill, the person shall be considered a health information trustee for purposes of this part. The person shall be subject to subpart E (relating to enforcement) with respect to any such duty that the person fails to fulfill.

(3) EFFECT ON TRUSTEE.—An agreement or relationship with an affiliated person does not relieve a health information trustee of any duty or liability under this part.

(c) AUTHORITIES OF AFFILIATED PERSONS.—

(1) IN GENERAL.—An affiliated person may only exercise an authority under this part that the health information trustee with whom the person is affiliated may exercise and that the person has been given by the trustee pursuant to an agreement or relationship described in section 5120(c)(1)(C). With respect to any such authority, the person shall be considered a health information trustee for purposes of this part. The person shall be subject to subpart E (relating to enforcement) with respect to any act that exceeds such authority.

(2) EFFECT ON TRUSTEE.—An agreement or relationship with an affiliated person does not affect the authority of a health information trustee under this part.

SEC. 5165. AGENTS AND ATTORNEYS.

(a) IN GENERAL.—Except as provided in subsections (b) and (c), a person who is authorized by law (on grounds other than an individual's minority), or by an instrument recognized under law, to act as an agent, attorney, proxy, or other legal representative for a protected individual or the estate of a protected individual, or otherwise to exercise the rights of the individual or estate, may, to the extent authorized, exercise and discharge the rights of the individual or estate under this part.

(b) HEALTH CARE POWER OF ATTORNEY.—A person who is authorized by law (on grounds other than an individual's minority), or by an instrument recognized under law, to make decisions about the provision of health care to an individual who is incapacitated may exercise and discharge the rights of the individual under this part to the extent necessary to effectuate the terms or purposes of the grant of authority.

(c) NO COURT DECLARATION.—If a health care provider determines that an individual, who has not been declared

to be legally incompetent, suffers from a medical condition that prevents the individual from acting knowingly or effectively on the individual's own behalf, the right of the individual to authorize disclosure under section 5132 may be exercised and discharged in the best interest of the individual by—

(1) a person described in subsection (b) with respect to the individual;

(2) a person described in subsection (a) with respect to the individual, but only if a person described in paragraph (1) cannot be contacted after a reasonable effort;

(3) the next of kin of the individual, but only if a person described in paragraph (1) or (2) cannot be contacted after a reasonable effort; or

(4) the health care provider, but only if a person described in paragraph (1), (2), or (3) cannot be contacted after a reasonable effort.

SEC. 5166. MINORS.

(a) INDIVIDUALS WHO ARE 18 OR LEGALLY CAPABLE.—In the case of an individual—

(1) who is 18 years of age or older, all rights of the individual shall be exercised by the individual, except as provided in section 5165; or

(2) who, acting alone, has the legal capacity to apply for and obtain health care and has sought such care, the individual shall exercise all rights of an individual under this part with respect to protected health information relating to such care.

(b) INDIVIDUALS UNDER 18.—Except as provided in subsection (a)(2), in the case of an individual who is—

(1) under 14 years of age, all the individual's rights under this part shall be exercised through the parent or legal guardian of the individual; or

(2) 14, 15, 16, or 17 years of age, the right of inspection (under section 5121), the right of amendment (under section 5122), and the right to authorize disclosure of protected health information (under section 5132) of the individual may be exercised either by the individual or by the parent or legal guardian of the individual.

SEC. 5167. MAINTENANCE OF CERTAIN PROTECTED HEALTH INFORMATION.

(a) IN GENERAL.—A State shall establish a process under which the protected health information described in subsection (b) that is maintained by a person described in subsection (c) is delivered to, and maintained by, the State or an individual or entity designated by the State.

(b) INFORMATION DESCRIBED.—The protected health information referred to in subsection (a) is protected health information that—

(1) is recorded in any form or medium;

(2) is created by—

(A) a health care provider; or

(B) a health benefit plan sponsor that provides benefits in the form of items and services to enrollees and not in the form of reimbursement for items and services; and

(3) relates in any way to the past, present, or future physical or mental health or condition or functional status of a protected individual or the provision of health care to a protected individual.

(c) PERSONS DESCRIBED.—A person referred to in subsection (a) is any of the following:

(A) A health care facility previously located in the State that has closed.

(B) A professional practice previously operated by a health care provider in the State that has closed.

(C) A health benefit plan sponsor that—

(i) previously provided benefits in the form of items and services to enrollees in the State; and

(ii) has ceased to do business.

Subpart E—Enforcement

SEC. 5171. CIVIL ACTIONS.

(a) IN GENERAL.—Any individual whose right under this part has been knowingly or negligently violated—

(1) by a health information trustee, or any other person, who is not described in paragraph (2), (3), (4), or (5) may maintain a civil action for actual damages and for equitable relief against the health information trustee or other person;

(2) by an officer or employee of the United States while the officer or employee was acting within the scope of the office or employment may maintain a civil action for actual damages and for equitable relief against the United States;

(3) by an officer or employee of any government authority of a State that has waived its sovereign immunity to a claim for damages resulting from a violation of this part while the officer or employee was acting within the scope of the office or employment may maintain a civil action for actual damages and for equitable relief against the State government;

(4) by an officer or employee of a government of a State that is not described in paragraph (3) may maintain a civil action for actual damages and for equitable relief against the officer or employee; or

(5) by an officer or employee of a government authority while the officer or employee was not acting within the scope of the office or employment may maintain a civil action for actual damages and for equitable relief against the officer or employee.

(b) KNOWING VIOLATIONS.—Any individual entitled to recover actual damages under this section because of a knowing violation of a provision of this part (other than subsection (c) or (d) of section 5131) shall be entitled to recover the amount of the actual damages demonstrated or $5000, whichever is greater.

(c) ACTUAL DAMAGES.—For purposes of this section, the term "actual damages" includes damages paid to compensate an individual for nonpecuniary losses such as physical and mental injury as well as damages paid to compensate for pecuniary losses.

(d) PUNITIVE DAMAGES; ATTORNEY'S FEES.—In any action brought under this section in which the complainant has prevailed because of a knowing violation of a provision of this part (other than subsection (c) or (d) of section 5131), the court may, in addition to any relief awarded under subsections (a) and (b), award such punitive damages as may be warranted. In such an action, the court, in its discretion, may allow the prevailing party a reasonable attorney's fee (including expert fees) as part of the costs, and the United States shall be liable for costs the same as a private person.

(e) LIMITATION.—A civil action under this section may not be commenced more than 2 years after the date on which the aggrieved individual discovered the violation or the date on which the aggrieved individual had a reasonable opportunity to discover the violation, whichever occurs first.

(f) INSPECTION AND AMENDMENT.—If a health information trustee has established a formal internal procedure that allows an individual who has been denied inspection or amendment of protected health information to appeal the denial, the individual may not maintain a civil action in connection with the denial until the earlier of—

(1) the date the appeal procedure has been exhausted; or

(2) the date that is 4 months after the date on which the appeal procedure was initiated.

(g) NO LIABILITY FOR PERMISSIBLE DISCLOSURES.—A health information trustee who makes a disclosure of protected health information about a protected individual that is permitted by this part and not otherwise prohibited by State or Federal statute shall not be liable to the individual for the disclosure under common law.

(h) NO LIABILITY FOR INSTITUTIONAL REVIEW BOARD DETERMINATIONS.—If the members of a certified institutional review board have in good faith determined that an approved health research project is of sufficient importance so as to outweigh the intrusion into the privacy of an individual pursuant to section 5136(a)(1), the members, the board, and the parent institution of the board shall not be liable to the individual as a result of such determination.

(i) GOOD FAITH RELIANCE ON CERTIFICATION.—A health information trustee who relies in good faith on a certifi-

cation by a government authority or other person and discloses protected health information about an individual in accordance with this part shall not be liable to the individual for such disclosure.

SEC. 5172. CIVIL MONEY PENALTIES.

(a) VIOLATION.—Any health information trustee who the Secretary determines has demonstrated a pattern or practice of failure to comply with the provisions of this part shall be subject, in addition to any other penalties that may be prescribed by law, to a civil money penalty of not more than $10,000 for each such failure. In determining the amount of any penalty to be assessed under the procedures established under subsection (b), the Secretary shall take into account the previous record of compliance of the person being assessed with the applicable requirements of this part and the gravity of the violation.

(b) PROCEDURES FOR IMPOSITION OF PENALTIES.—The provisions of section 1128A of the Social Security Act (other than subsections (a) and (b)) shall apply to the imposition of a civil monetary penalty under this section in the same manner as such provisions apply with respect to the imposition of a penalty under section 1128A of such Act.

SEC. 5173. ALTERNATIVE DISPUTE RESOLUTION.

(a) IN GENERAL.—Not later than July 1, 1996, the Secretary shall, by regulation, develop alternative dispute resolution methods for use by individuals, health information trustees, and other persons in resolving claims under section 5171.

(b) EFFECT ON INITIATION OF CIVIL ACTIONS.—

(1) IN GENERAL.—Subject to paragraph (2), the regulations established under subsection (a) may provide that an individual alleging that a right of the individual under this part has been violated shall pursue at least one alternative dispute resolution method developed under such subsection as a condition precedent to commencing a civil action under section 5171.

(2) LIMITATION.—Such regulations may not require an individual to refrain from commencing a civil action to pursue one or more alternative dispute resolution method for a period that is greater than 6 months.

(3) SUSPENSION OF STATUTE OF LIMITATIONS.—The regulations established by the Secretary under subsection (a) may provide that a period in which an individual described in paragraph (1) pursues (as defined by the Secretary) an alternative dispute resolution method under this section shall be excluded in computing the period of limitations under section 5171(e).

(c) METHODS.—The methods under subsection (a) shall include at least the following:

(1) ARBITRATION.—The use of arbitration.

(2) MEDIATION.—The use of mediation.

(3) EARLY OFFERS OF SETTLEMENT.—The use of a process under which parties make early offers of settlement.

(d) STANDARDS FOR ESTABLISHING METHODS.—In developing alternative dispute resolution methods under subsection (a), the Secretary shall ensure that the methods promote the resolution of claims in a manner that—

(1) is affordable for the parties involved;

(2) provides for timely and fair resolution of claims; and

(3) provides for reasonably convenient access to dispute resolution for individuals.

SEC. 5174. AMENDMENTS TO CRIMINAL LAW.

(a) IN GENERAL.—Title 18, United States Code, is amended by inserting after chapter 89 the following:

"CHAPTER 90—PROTECTED HEALTH INFORMATION

"§ 1831. Definitions

"As used in this chapter—

"(1) the term 'health information trustee' has the meaning given such term in section 5120(b)(6) of the Health Security Act;

"(2) the term 'protected health information' has the meaning given such term in section 5120(a)(3) of such Act; and

"(3) the term 'protected individual' has the meaning given such term in section 5120(a)(4) of such Act.

"§ 1832. Obtaining protected health information under false pretenses

"Whoever under false pretenses—

"(1) requests or obtains protected health information from a health information trustee; or

"(2) obtains from a protected individual an authorization for the disclosure of protected health information about the individual maintained by a health information trustee;

shall be fined under this title or imprisoned not more than 5 years, or both.

"§ 1833. Monetary gain from obtaining protected health information under false pretenses

"Whoever under false pretenses—

"(1) requests or obtains protected health information from a health information trustee with the intent to sell, transfer, or use such information for profit or monetary gain; or

"(2) obtains from a protected individual an authorization for the disclosure of protected health information about the individual maintained by a health information trustee with the intent to sell, transfer, or use such authorization for profit or monetary gain;

and knowingly sells, transfers, or uses such information or authorization for profit or monetary gain shall be fined under this title or imprisoned not more than 10 years, or both.

"§ 1834. Knowing and unlawful obtaining of protected health information

"Whoever knowingly obtains protected health information from a health information trustee in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such obtaining is unlawful, shall be fined under this title or imprisoned not more than 5 years, or both.

"§ 1835. Monetary gain from knowing and unlawful obtaining of protected health information

"Whoever knowingly—

"(1) obtains protected health information from a health information trustee in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such obtaining is unlawful and with the intent to sell, transfer, or use such information for profit or monetary gain; and

"(2) knowingly sells, transfers, or uses such information for profit or monetary gain;

shall be fined under this title or imprisoned not more than 10 years, or both.

"§ 1836. Knowing and unlawful use or disclosure of protected health information

"Whoever knowingly uses or discloses protected health information in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such use or disclosure is unlawful, shall be fined under this title or imprisoned not more than 5 years, or both.

"§ 1837. Monetary gain from knowing and unlawful sale, transfer, or use of protected health information

"Whoever knowingly sells, transfers, or uses protected health information in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such sale,

transfer, or use is unlawful, shall be fined under this title or imprisoned not more than 10 years, or both.".

(b) CLERICAL AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following:

"90. Protected health information ..... 1831".

Subpart F—Amendments to Title 5, United States Code

SEC. 5181. AMENDMENTS TO TITLE 5, UNITED STATES CODE.

(a) NEW SUBSECTION.—Section 552a of title 5, United States Code, is amended by adding at the end the following:

"(w) MEDICAL EXEMPTIONS.—The head of an agency that is a health information trustee (as defined in section 5120(b)(6) of the Health Security Act) shall promulgate rules, in accordance with the requirements (including general notice) of subsections (b)(1), (b)(2), (b)(3), (c), and (e) of section 553 of this title, to exempt a system of records within the agency, to the extent that the system of records contains protected health information (as defined in section 5120(a)(3) of such Act), from all provisions of this section except subsections (e)(1), (e)(2), subparagraphs (A) through (C) and (E) through (I) of subsection (e)(4), and subsections (e)(5), (e)(6), (e)(9), (e)(12), (l), (n), (o), (p), (q), (r), and (u).".

(b) REPEAL.—Section 552a(f)(3) of title 5, United States Code, is amended by striking "pertaining to him," and all that follows through the semicolon and inserting "pertaining to the individual;".

Subpart G—Regulations, Research, and Education; Effective Dates; Applicability; and Relationship to Other Laws

SEC. 5191. REGULATIONS; RESEARCH AND EDUCATION.

(a) REGULATIONS.—Not later than July 1, 1996, the Secretary shall prescribe regulations to carry out this part.

(b) RESEARCH AND TECHNICAL SUPPORT.—The Secretary may sponsor—

(1) research relating to the privacy and security of protected health information;

(2) the development of consent forms governing disclosure of such information; and

(3) the development of technology to implement standards regarding such information.

(c) EDUCATION.—The Secretary shall establish education and awareness programs—

(1) to foster adequate security practices by health information trustees;

(2) to train personnel of health information trustees respecting the duties of such personnel with respect to protected health information; and

(3) to inform individuals and employers who purchase health care respecting their rights with respect to such information.

SEC. 5192. EFFECTIVE DATES.

(a) IN GENERAL.—Except as provided in subsection (b), this part, and the amendments made by this part, shall take effect on January 1, 1997.

(b) PROVISIONS EFFECTIVE IMMEDIATELY.—A provision of this part shall take effect on the date of the enactment of this Act if the provision—

(1) imposes a duty on the Secretary to develop, establish, or promulgate regulations, guidelines, notices, statements, or education and awareness programs; or

(2) authorizes the Secretary to sponsor research or the development of forms or technology.

SEC. 5193. APPLICABILITY.

(a) PROTECTED HEALTH INFORMATION.—Except as provided in subsections (b) and (c), the provisions of this part shall apply to any protected health information that is received, created, used, maintained, or disclosed by a health information trustee in a State on or after January 1, 1997, regardless of whether the information existed or was disclosed prior to such date.

(b) EXCEPTION.—

(1) IN GENERAL.—The provisions of this part shall not apply to a trustee described in paragraph (2), except with respect to protected health information that is received by the trustee on or after January 1, 1997.

(2) APPLICABILITY.—A trustee referred to in paragraph (1) is—

(A) a health researcher; or

(B) a person who, with respect to specific protected health information, received the information—

(i) pursuant to—

(I) section 5137 (relating to emergency circumstances);

(II) section 5138 (relating to judicial and administrative purposes);

(III) section 5139 (relating to law enforcement); or

(IV) section 5140 (relating to subpoenas, warrants, and search warrants); or

(ii) while acting in whole or in part in the capacity of an officer or employee of a person described in clause (i).

(c) AUTHORIZATIONS FOR DISCLOSURES.—An authorization for the disclosure of protected health information about a protected individual that is executed by the individual before January 1, 1997, and is recognized and valid

under State law on December 31, 1996, shall remain valid and shall not be subject to the requirements of section 5132 until January 1, 1998, or the occurrence of the date or event (if any) specified in the authorization upon which the authorization expires, whichever occurs earlier.

SEC. 5194. RELATIONSHIP TO OTHER LAWS.

(a) STATE LAW.—Except as otherwise provided in subsections (b), (c), (d), and (f), a State may not establish, continue in effect, or enforce any State law to the extent that the law is inconsistent with, or imposes additional requirements with respect to, any of the following:

(1) A duty of a health information trustee under this part.

(2) An authority of a health information trustee under this part to disclose protected health information.

(3) A provision of subpart C (relating to access procedures and challenge rights), subpart D (miscellaneous provisions), or subpart (E) (relating to enforcement).

(b) LAWS RELATING TO PUBLIC HEALTH AND MENTAL HEALTH.—This part does not preempt, supersede, or modify the operation of any State law regarding public health or mental health to the extent that the law prohibits or regulates a disclosure of protected health information that is permitted under this part.

(c) CRIMINAL PENALTIES.—A State may establish and enforce criminal penalties with respect to a failure to comply with a provision of this part.

(d) PRIVILEGES.—A privilege that a person has under law in a court of a State or the United States or under the rules of any agency of a State or the United States may not be diminished, waived, or otherwise affected by—

(1) the execution by a protected individual of an authorization for disclosure of protected health information under this part, if the authorization is executed for the purpose of receiving health care or providing for the payment for health care; or

(2) any provision of this part that authorizes the disclosure of protected health information for the purpose of receiving health care or providing for the payment for health care.

(e) DEPARTMENT OF VETERANS AFFAIRS.—The limitations on use and disclosure of protected health information under this part shall not be construed to prevent any exchange of such information within and among components of the Department of Veterans Affairs that determine eligibility for or entitlement to, or that provide, benefits under laws administered by the Secretary of Veterans Affairs.

(f) CERTAIN DUTIES UNDER STATE OR FEDERAL LAW.—This part shall not be construed to preempt, supersede, or modify the operation of any of the following:

(1) Any law that provides for the reporting of vital statistics such as birth or death information.

(2) Any law requiring the reporting of abuse or neglect information about any individual.

(3) Subpart II of part E of title XXVI of the Public Health Service Act (relating to notifications of emergency response employees of possible exposure to infectious diseases).

(4) The Americans with Disabilities Act of 1990.

(5) Any Federal or State statute that establishes a privilege for records used in health professional peer review activities.

(g) SECRETARIAL AUTHORITY.—

(1) SECRETARY OF HEALTH AND HUMAN SERVICES.—A provision of this part does not preempt, supersede, or modify the operation of section 543 of the Public Health Service Act, except to the extent that the Secretary of Health and Human Services determines through regulations promulgated by such Secretary that the provision provides greater protection for protected health information, and the rights of protected individuals, than is provided under such section 543.

(2) SECRETARY OF VETERANS AFFAIRS.—A provision of this part does not preempt, supersede, or modify the operation of section 7332 of title 38, United States Code, except to the extent that the Secretary of Veterans Affairs determines through regulations promulgated by such Secretary that the provision provides greater protection for protected health information, and the rights of protected individuals, than is provided under such section 7332.

Page 860, line 9, strike "section 5120" and insert "part 2".

Page 867, strike lines 4 through 10.

Page 867, beginning on line 22, strike "individually" through "5123(3))" on line 23 and insert "protected health information (as defined in section 5120(a)(3))".

Page 867, beginning on line 25, strike "individually identifiable information" and insert "protected health information".

Page 883, line 8, strike "with respect to its duties" and insert "and the Secretary with respect to the respective duties of the Board and the Secretary".

Page 883, line 11, strike "Board." and insert "Board, in consultation with the Secretary.".

Page 885, line 16, strike "5101 or 5120;" and insert "5101;".

Beginning on page 886, strike line 17 through page 887, line 2 (and conform the table of contents for title V accordingly).

Amend section 5401 (page 948, line 5 through page 951, line 3) to read as follows (and conform the table of contents for title V accordingly):

SEC. 5401. HEALTH CARE FRAUD AND ABUSE.

(a) FEDERAL ENFORCEMENT BY INSPECTORS GENERAL AND ATTORNEY GENERAL.—

(1) AUDITS, INVESTIGATIONS, INSPECTIONS, AND EVALUATIONS.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the Inspector General of each of the Department of Health and Human Services, the Department of Defense, the Department of Labor, the Office of Personnel Management, and the Department of Veterans Affairs, and the Attorney General shall conduct audits, civil and criminal investigations, inspections, and evaluations relating to the prevention, detection, and control of health care fraud and abuse in violation of any Federal law.

(B) LIMITATION.—An Inspector General, other than the Inspector General of the Department of Health and Human Services, may not conduct any audit, investigation, inspection, or evaluation under subparagraph (A) with respect to health care fraud or abuse under title V, XI, XVIII, XIX, or XX of the Social Security Act.

(2) POWERS.—For purposes of carrying out duties and responsibilities under paragraph (1), each Inspector General referred to in paragraph (1) may exercise powers that are available to the Inspector General for purposes of audits, investigations, and other activities under the Inspector General Act of 1978 (5 U.S.C. App.).

(3) COORDINATION AND REVIEW OF ACTIVITIES OF OTHER FEDERAL, STATE, AND LOCAL AGENCIES.—

(A) PROGRAM.—The Inspector General and the Attorney General shall—

(i) jointly establish, on the effective date specified in subsection (j)(1), a program to prevent, detect, and control health care fraud and abuse in violation of any Federal law, which considers the activities of Federal, State, and local law enforcement agencies, Federal and State agencies responsible for the licensing and certification of health care providers, and State agencies designated under subsection (b)(1)(A); and

(ii) publish a description of the program in the Federal Register, by not later than June 30, 1995.

(B) ANNUAL INVESTIGATIVE PLAN.—Each Inspector General referred to in paragraph (1) and the Attorney General shall each develop an annual in-

vestigative plan for the prevention, detection, and control of health care fraud and abuse in accordance with the program established under subparagraph (A).

(4) CONSULTATIONS.—Each of the Inspectors General referred to in paragraph (1) and the Attorney General shall regularly consult with each other, with Federal, State, and local law enforcement agencies, with Federal and State agencies responsible for the licensing and certification of health care providers, and with Health Care Fraud and Abuse Control Units, in order to assist in coordinating the prevention, detection, and control of health care fraud and abuse in violation of any Federal law.

(b) STATE ENFORCEMENT.—

(1) DESIGNATION OF STATE AGENCIES AND ESTABLISHMENT OF HEALTH CARE FRAUD AND ABUSE CONTROL UNIT.—The Governor of each State—

(A) shall, consistent with State law, designate agencies of the State which conduct, supervise, and coordinate audits, civil and criminal investigations, inspections, and evaluations relating to the prevention, detection, and control of health care fraud and abuse in violation of any Federal law in the State; and

(B) may establish and maintain in accordance with paragraph (2) a State agency to act as a Health Care Fraud and Abuse Control Unit for purposes of this section.

(2) HEALTH CARE FRAUD AND ABUSE CONTROL UNIT REQUIREMENTS.—A Health Care Fraud and Abuse Control Unit established by a State under paragraph (1)(B) shall be a single identifiable entity of State government which is separate and distinct from any State agency with principal responsibility for the administration of health care programs, and which meets the following requirements:

(A) The entity—

(i) is a unit of the office of the State Attorney General or of another department of State government that possesses statewide authority to prosecute individuals for criminal violations;

(ii) is in a State the constitution of which does not provide for the criminal prosecution of individuals by a statewide authority, and has formal procedures, approved by the Secretary, that assure it will refer suspected criminal violations relating to health care fraud or abuse in violation of any Federal law to the appropriate authority or authorities of the State for prosecution and assure it will assist such authority or authorities in such prosecutions; or

(iii) has a formal working relationship with the office of the State Attorney General or the appropriate authority or authorities for prosecution and has formal procedures (including procedures under which it will refer suspected criminal violations to such office), that provide effective coordination of activities between the Health Care Fraud and Abuse Control Unit and such office with respect to the detection, investigation, and prosecution of suspected health care fraud or abuse in violation of any Federal law.

(B) The entity conducts a statewide program for the investigation and prosecution of violations of all applicable State laws regarding any and all aspects of health care fraud and abuse in violation of any Federal law.

(C) The entity has procedures for—

(i) reviewing complaints of the abuse or neglect of patients of health care facilities in the State, and

(ii) where appropriate, investigating and prosecuting such complaints under the criminal laws of the State or for referring the complaints to other State or Federal agencies for action.

(D) The entity provides for the collection, or referral for collection to the appropriate agency, of overpayments that—

(i) are made under any federally funded or mandated health care program required by this Act, and

(ii) it discovers in carrying out its activities.

(E) The entity employs attorneys, auditors, investigators, and other necessary personnel, is organized in such a manner, and provides sufficient resources, as is necessary to promote the effective and efficient conduct of its activities.

(3) SUBMISSION OF ANNUAL PLAN.—Each Health Care Fraud and Abuse Control Unit may submit each year to the Inspector General and the Attorney General a plan for preventing, detecting, and controlling, consistent with the program established under subsection (a)(3)(A), health care fraud and abuse in violation of any Federal law.

(4) APPROVAL OF ANNUAL PLAN.—The Inspector General shall approve a plan submitted under paragraph (3) by the Health Care Fraud and Abuse Control Unit of a State, unless the Inspector General establishes that the plan—

(A) is inconsistent with the program established under subsection (a)(3)(A); or

(B) will not enable the agencies of the State designated under paragraph (1)(A) to prevent, detect,

and control health care fraud and abuse in violation of any Federal law.

(5) REPORTS.—Each Health Care Fraud and Abuse Control Unit shall submit to the Inspector General an annual report containing such information as the Inspector General determines to be necessary.

(6) SEMIANNUAL REPORTS OF INSPECTOR GENERAL OF HEALTH AND HUMAN SERVICES.—The Inspector General shall include in each semiannual report of the Inspector General to the Congress under section 5(a) of the Inspector General Act of 1978 (5 U.S.C. App.) an assessment of the Inspector General of how well States are preventing, detecting, and controlling health care fraud and abuse.

(c) PAYMENTS TO STATES.—

(1) IN GENERAL.—For each year for which a State has a plan approved under subsection (b)(4), and subject to the availability of appropriations, the Inspector General shall pay to the State for each quarter an amount equal to 75 percent of the sums expended during the quarter by agencies designated by the Governor of the State under subsection (b)(1)(A) in conducting activities described in that subsection.

(2) TIME OF PAYMENT.—The Inspector General shall make a payment under paragraph (1) for a quarter by not later than 30 days after the end of the quarter.

(3) PAYMENTS ARE ADDITIONAL.—Payments to a State under this subsection shall be in addition to any amounts paid under subsection (g).

(d) DATA SHARING.—The Inspector General and the Attorney General shall jointly establish a program for the sharing among Federal agencies, State and local law enforcement agencies, and health care providers and insurers, consistent with data sharing provisions of subtitle B, of data related to possible health care fraud and abuse in violation of any Federal law.

(e) HEALTH CARE FRAUD AND ABUSE CONTROL ACCOUNT.—

(1) ESTABLISHMENT.—There is established on the books of the Treasury of the United States a separate account, which shall be known as the Health Care Fraud and Abuse Control Account. The Account shall consist of—

(A) the Health Care Fraud and Abuse Expenses Subaccount; and

(B) the Health Care Fraud and Abuse Reserve Subaccount.

(2) EXPENSES SUBACCOUNT.—

(A) CONTENTS.—The Expenses Subaccount consists of—

(i) amounts deposited under subparagraph (B); and

(ii) amounts transferred from the Reserve Subaccount and deposited under paragraph (3)(B).

(B) DEPOSITS.—Except as provided in paragraph (3)(A), there shall be deposited in the Expenses Subaccount all amounts received by the United States as—

(i) fines for health care fraud and abuse in violation of any Federal law;

(ii) civil penalties or damages (other than restitution) in actions under section 3729 or 3730 of title 31, United States Code (commonly referred to as the "False Claims Act"), that are based on health care fraud and abuse in violation of any Federal law;

(iii) administrative penalties under the Social Security Act;

(iv) proceeds of seizures and forfeitures of property for acts or omissions that constitute health care fraud or abuse in violation of any Federal law; and

(v) money and proceeds of property that are accepted under subsection (f).

(C) USE.—Amounts in the Expenses Subaccount shall be available to the Inspector General and the Attorney General, under such terms and conditions as the Inspector General and the Attorney General jointly determine to be appropriate, for—

(i) paying expenses incurred by their respective agencies in carrying out activities under subsection (a); and

(ii) making reimbursements to other Inspectors General and Federal, State, and local agencies in accordance with subsection (g).

(3) RESERVE SUBACCOUNT.—

(A) DEPOSITS.—An amount otherwise required under paragraph (2)(A) to be deposited in the Expenses Subaccount in a fiscal year shall be deposited in the Reserve Subaccount, if—

(i) the amount in the Expenses Subaccount is greater than $500,000,000; and

(ii) the deposit of that amount in the Expenses Subaccount would result in the amount in the Expenses Subaccount exceeding 110 percent of the total amount deposited in the Expenses Subaccount in the preceding fiscal year.

(B) TRANSFERS TO EXPENSES SUBACCOUNT.—

(i) ESTIMATION OF SHORTFALL.—Not later than the first day of the last quarter of each fiscal year, the Inspector General (in consultation with the Attorney General) shall estimate whether sufficient amounts will be available during such quarter in the Expenses Sub-

account for the uses described in paragraph (2)(C).

(ii) TRANSFER TO COVER SHORTFALL.—If the Inspector General estimates under clause (i) that there will not be available sufficient amounts in the Expenses Subaccount during the last quarter of a fiscal year, there shall be transferred from the Reserve Subaccount and deposited in the Expenses Subaccount such amount as the Inspector General estimates is required to ensure that sufficient amounts are available in the Expenses Subaccount during such quarter.

(C) LIMITATION ON AMOUNT CARRIED OVER TO SUCCEEDING FISCAL YEAR.—There shall be transferred to the general fund of the Treasury any amount remaining in the Reserve Subaccount at the end of a fiscal year (after any transfer made under subparagraph (B)) in excess of 10 percent of the total amount authorized to be deposited in the Expenses Subaccount (consistent with subparagraph (A)) during the fiscal year.

(f) ACCEPTANCE OF GIFTS, BEQUESTS, AND DEVISES.—The Attorney General or any Inspector General referred to in subsection (a)(1) may accept, use, and dispose of gifts, bequests, or devises of services or property (real or personal), for the purpose of aiding or facilitating activities under this section regarding health care fraud and abuse. Gifts, bequests, or devises of money and proceeds from sales of other property received as gifts, bequests, or devises shall be deposited in the Account and shall be available for use in accordance with subsection (e)(2)(C).

(g) REIMBURSEMENTS OF EXPENSES AND OTHER PAYMENTS TO PARTICIPATING AGENCIES.—

(1) REIMBURSEMENT OF EXPENSES OF FEDERAL AGENCIES.—The Inspector General and the Attorney General, subject to the availability of amounts in the Account, shall jointly and promptly reimburse Federal agencies for expenses incurred in carrying out subsection (a).

(2) PAYMENTS TO STATE AND LOCAL LAW ENFORCEMENT AGENCIES.—The Inspector General and the Attorney General, subject to the availability of amounts in the Account, shall jointly and promptly pay to any State or local law enforcement agency that participated directly in any activity which led to deposits in the Account, or property the proceeds of which are deposited in the Account, an amount that reflects generally and equitably the participation of the agency in the activity.

(3) FUNDS USED TO SUPPLEMENT AGENCY APPROPRIATIONS.—It is intended that disbursements made from the Account to any Federal agency be used to increase

and not supplant the recipient agency's appropriated operating budget.

(h) ACCOUNT PAYMENTS ADVISORY BOARD.—

(1) ESTABLISHMENT.—There is established the Account Payments Advisory Board, which shall make recommendations to the Inspector General and the Attorney General regarding the equitable allocation of payments from the Account.

(2) MEMBERSHIP.—The Board shall consist of—

(A) each of the Inspectors General referred to in subsection (a)(1), other than the Inspector General of the Department of Health and Human Services; and

(B) 10 members appointed by the Inspector General of the Department of Health and Human Services to represent Health Care Fraud and Abuse Control Units, of whom one shall be appointed—

(i) for each of the 10 regions established by the Director of the Office of Management and Budget under Office of Management and Budget Circular A–105, to represent Units in that region; and

(ii) from among individuals recommended by the heads of those agencies in that region.

(3) TERMS.—The term of a member of the Board appointed under paragraph (2)(B) shall be 3 years, except that of such members first appointed 3 members shall serve an initial term of one year and 3 members shall serve an initial term of 2 years, as specified by the Inspector General at the time of appointment.

(4) VACANCIES.—A vacancy on the Board shall be filled in the same manner in which the original appointment was made, except that an individual appointed to fill a vacancy occurring before the expiration of the term for which the individual is appointed shall be appointed only for the remainder of that term.

(5) CHAIRPERSON AND BYLAWS.—The Board shall elect one of its members as chairperson and shall adopt bylaws.

(6) COMPENSATION AND EXPENSES.—Members of the Board shall serve without compensation, except that the Inspector General may pay the expenses reasonably incurred by the Board in carrying out its functions under this section.

(7) NO TERMINATION.—Section 14(a)(2) of the Federal Advisory Committee Act (5 U.S.C. App.) does not apply to the Board.

(i) DEFINITIONS.—In this section:

(1) ACCOUNT.—The term "Account" means the Health Care Fraud and Abuse Control Account established by subsection (e)(1).

(2) EXPENSES SUBACCOUNT.—The term "Expenses Subaccount" means the Health Care Fraud and Abuse Expenses Subaccount of the Account.

(3) HEALTH CARE FRAUD AND ABUSE CONTROL UNIT.—The term "Health Care Fraud and Abuse Control Unit" means such a unit established by a State in accordance with subsection (b)(2).

(4) INSPECTOR GENERAL.—Except as otherwise provided, the term "Inspector General" means the Inspector General of the Department of Health and Human Services

(5) RESERVE SUBACCOUNT.—The term "Reserve Subaccount" means the Health Care Fraud and Abuse Reserve Subaccount of the Account.

(j) EFFECTIVE DATE.—

(1) IN GENERAL.—Except as provided in paragraph (2), this section shall take effect on January 1, 1996.

(2) DEVELOPMENT AND PUBLICATION OF DESCRIPTION OF PROGRAM.—Subsection (a)(3)(A) shall take effect on the date of the enactment of this Act.

REPORT ON SUBTITLE B OF TITLE V

PURPOSE AND SUMMARY—FAIR HEALTH INFORMATION PRACTICES

The purpose of the Fair Health Information Practices Part of the Health Security Act is to establish a code of fair information practices for health information that originates in or becomes a part of the health treatment or payment system. The part establishes uniform federal rules that will apply to covered health information in all states.

There are two basic concepts in the Act. Identifiable health information that is created or used during the health treatment or payment process is protected health information. In general, protected health information remains subject to statutory restriction no matter how it is used or disclosed.

The second basic concept is that of a health information trustee. Almost everyone who has access to protected health information becomes a health information trustee under the part. Health care providers, benefit plans and carriers, oversight agencies, and public health authorities are health information trustees. Others who obtain protected health information infrequently—such as health researchers and law enforcement agencies—are also health information trustees.

The responsibilities and authorities for each trustee have been carefully defined to balance each individual's right to privacy and the need for confidentiality in the health treatment process against legitimate societal needs such as public health, health research, cost containment, and law enforcement. Trustees are required to—

limit disclosure of protected health information to the minimum necessary to accomplish the purpose;

use protected health information only for a purpose that is compatible with and directly related to the purpose for which the information was collected or obtained by the trustee;

maintain appropriate administrative, technical, and physical safeguards to protect integrity and privacy of health information;

disclose protected health information only for an authorized purpose; and

maintain an accounting of the date, nature, and purpose of any disclosure of protected health information.

Individual rights vary slightly depending on which trustee maintains protected health information. For health information used in treatment, payment, or oversight, individuals have the right to—

inspect and have a copy of their health information;

seek correction of health information that is not timely, accurate, relevant, or complete; and

receive a notice explaining their rights and how their information may be used.

The Fair Health Information Practices Part includes several enforcement mechanisms, including criminal penalties (up to ten years in prison), civil remedies, and civil money penalties that may be imposed by the Secretary of Health and Human Services. In addition, the part provides for alternate dispute resolution as another mechanism for resolving disputes.

The Fair Health Information Practices Part is based on the Fair Health Information Practices Act of 1994 (H.R. 4077) which was introduced on March 17, 1994, by Rep. Gary Condit, Chairman of the Subcommittee on Information, Justice, Transportation, and Agriculture.

BACKGROUND AND NEED FOR FAIR HEALTH INFORMATION PRACTICES [1]

Right to privacy

There is no doubt about the views of the public on the importance of privacy of health records. A recent poll conducted by Louis Harris and Associates for Equifax, Inc., found that an overwhelming majority (eighty-five percent) of the public believe that protecting the confidentiality of health records is absolutely essential or very important in national health care reform. According to Dr. Alan Westin, the public put this priority even ahead of reform goals such as providing health insurance for those who do not have it, reducing paperwork burdens on patients and providers, and obtaining better data for medical research.[2]

The basic constitutional principles of individual privacy were well stated over fifty years ago by Justice Brandeis in his famous dissent in *Olmstead* v. *United States:*

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect * * *. They conferred, as against

[1] The Subcommittee on Information, Justice, Transportation, and Agriculture held four days of hearings on health care confidentiality issues. The first, titled "Health Reform, Health Records, Computers and Confidentiality", was held on November 4, 1993. The other three were legislative hearings on the Fair Health Information Practices Act of 1994 (H.R. 4077). The hearing dates were April 20, 1994; May 4, 1994; and May 5, 1994. The legislative hearings are hereinafter cited as "H.R. 4077 Hearings". All hearings will be printed.

[2] Testimony of Dr. Alan Westin, Professor of Public Law and Government, Columbia University, at H.R. 4077 Hearings (April 20, 1994). Dr. Westin was the academic advisor to the Harris-Equifax poll. See "Health Information Privacy Survey 1993."

> the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed must be deemed a violation of the fourth amendment.[3]

The view that privacy is a fundamental constitutional right was endorsed by the Congress in the Privacy Act of 1974, which included a specific finding that the "right to privacy is a personal and fundamental right protected by the Constitution of the United States."[4] In several decisions, the Supreme Court has recognized a constitutional right to privacy. Of particular relevance to a discussion of health records is *Whalen* v. *Roe*.[5] This case involved a New York State statute that required pharmacists and physicians to report the names of patients receiving certain types of prescription drugs to state officials. The law was found to be constitutional on two grounds: the societal interests served by the statute (fighting illegal use of legal drugs), and the extensive confidentiality protections included in the law. The case illustrates the types of compelling demands that can be placed on health information as well as the importance of confidentiality protections when sensitive health information is used for other purposes. The case also illustrates that protection of health records may raise constitutional issues and that whatever constitutional protection is available for health records is subject to a balance of interests.[6]

The Miller decision

There are clearly significant limitations on the constitutional right to privacy. Some of these limitations are well-illustrated by the 1976 Supreme Court decision in *United States* v. *Miller*[7], a case involving the ability of the government to obtain sensitive personal information from banks.

In *Miller,* the Supreme Court reaffirmed the traditional legal standard that a customer's account records in a bank are not the private papers of the customer. As a result, the individual has no legal right to challenge access to the records by the government or

---

[3] 277 U.S. 438 (1928)

[4] Public Law 93-579, § 2(a)(4), 5 U.S.C. § 552a note (1988).

[5] 429 U.S. 589 (1977).

[6] The Court concluded its opinion with these words: "A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces and the enforcement of the criminal laws, all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has it roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment." 429 U.S. 605–06 (footnote omitted). The Supreme Court also discussed the implications of computerized systems containing personal information in *Reporters Committee for Freedom of the Press* v. *Department of Justice,* 489 U.S. 749 (1989). See also the testimony of Professor Paul Schwartz in H.R. 4077 Hearings (May 4, 1994) (prepared statement at 12–13).

[7] 425 U.S. 435 (1976).

anyone else. A bank customer has no right to notice of a subpoena for the records of his or her account from a bank and no legal standing to protest the subpoena.

The stark significance of *Miller* becomes clearer in light of the change in the way that most people organize their financial affairs. Before checking accounts and credit cards were universally available, personal financial information was only available directly from the individual. When the individual under investigation by the government has the records being sought, the constitutional protections against governmental intrusion work well. Yet when that same information is held by a third party, such as a bank or credit grantor, the Supreme Court held that the individual has no protection against governmental intrusion, although the information is just as sensitive and just as personal. The result is that changes in technology, social and financial relationships, and information policy and practice have also changed the rights of citizens to control personal information.

Miller has no direct applicability to health records. Nevertheless, there is reason to believe that a case involving access to health records would have the same result. Robert Belair, then Counsel to the National Commission on Confidentiality of Health Records, testified that the Supreme Court might well see *Miller* as precedent for health records.[8] The Committee agrees that there is a substantial risk that *Miller* would be applied to health records. The Committee concludes that legislation to foreclose this possibility is essential.

This will not be the first time that Congress has acted to modify the effect of *Miller*. Based in part on a recommendation of the Privacy Protection Study Commission,[9] the 95th Congress enacted the Right to Financial Privacy Act.[10] This law protected the confidentiality of personal financial records maintained by financial institutions by limiting the ability of the federal government to obtain those records. The Right to Financial Privacy Act provides an individual with a right to notice and an opportunity to challenge a request from a federal agency for records about the individual held by a bank or other financial institution.[11] This was the first in a series of federal laws passed with the express purpose of limiting the effect of Miller.

The Cable Communications Policy Act of 1984[12] also took a cue from the recommendations of the Privacy Protection Study Commission regarding *Miller*.[13] The Act provides that a governmental entity may obtain individually identifiable information concerning a cable subscriber pursuant to court order only if the subject of the

---

[8] "Privacy of Medical Records," Hearings before a Subcomm. of the House Comm. on Government Operations, 96th Cong., 1st Sess. 238–239 (1979) [hereinafter cited as "1979 House Hearings"].

[9] Privacy Protection Study Commission, "Personal Privacy in an Information Society" (1977) [hereinafter cited as "PPSC Report"].

[10] Public Law 95–630, title XI, 92 Stat. 3697 (1978), 12 U.S.C. §3401–3421 (1988).

[11] Later amendments significantly weakened the limited privacy protections that were originally included in the Right to Financial Privacy Act.

[12] Public Law 98–549, 98 Stat. 2780 (1984).

[13] See House Comm. on Energy and Commerce, H.R. Rep. No. 98–934, 98th Cong., 2d Sess. 78–79 (1984) (report to accompany H.R. 4103).

information is afforded the opportunity to appear and contest the order.[14]

The Electronic Communications Privacy Act of 1986[15] was also passed with the intention of changing the effect of the *Miller* decision on customer records maintained by persons offering remote computing services.[16] This Act requires notice to the customer of a government subpoena for the contents of electronic communications in a remote computing service.[17]

The Video Privacy Protection Act of 1988[18] was passed to provide customers of video rental service providers with notice of a government warrant or subpoena for records in the possession of the providers.[19] This too was passed with an awareness of the recommendations of the Privacy Protection Study Commission that the *Miller* decision should be overturned.[20]

The Committee concludes that there is ample precedent for legislation overturning *Miller* for specific categories of records about individuals that are maintained by third party record keepers. The Committee also concludes that it is of the utmost importance that health records receive the highest degree of protection afforded to any category of personal records maintained by third party record keepers. There is no justification for having lesser privacy protections for medical records than for cable television or video rental records. While it is beyond the scope of the current legislation, there may be a need to reconsider the consequences of *Miller* for all personal information maintained by third party record keepers.

Secondary use of health information

A health record has become a rich repository of information for people and institutions who are not directly involved in the health treatment and payment process. Few patients or providers are aware of the extent of these secondary uses. According to one commentator:

> The value of medical information for uses outside the medical treatment and payment system has not been popularly recognized, and even medical professionals are largely unaware of the many uses to which the information may be put. Medical information increasingly is used to make nonmedical decisions about individuals as well as for purposes unrelated to the individuals who are the subject of the records.[21]

In a 1977 publication, the American Medical Record Association[22] identified twelve broad categories of social users and twenty-four ways that health information is used outside the treatment and payment process. The users are: public health agencies; medi-

---

[14] 47 U.S.C. §551(h)(2) (1988).
[15] Public Law 99–508, 100 Stat. 1848 (1986).
[16] House Comm. on the Judiciary, H.R. Rep. No. 99–647, 99th Cong., 2d Sess. 72–73 (1986) (report to accompany H.R. 4952).
[17] 18 U.S.C. §2703 (1988).
[18] Public Law 100–618, 102 Stat. 3195 (1988), 18 U.S.C. §2710 (1988).
[19] 18 U.S.C. §2709 (1988).
[20] Senate Comm. on the Judiciary, S. Rep. No. 100–599, 100th Cong., 2d Sess. 2–3 (1988) (report to accompany S. 2361).
[21] Gellman, "Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy," 62 North Carolina Law Review 255, 261 (1984) [hereinafter cited as "Gellman"].
[22] Now the American Health Information Management Association.

cal and social researchers; rehabilitation and social welfare programs; employers; insurance companies; federal, state, and local government agencies; education institutions; judicial institutions; law enforcement and investigation agencies; credit investigation agencies; accrediting, licensing and certifying organizations; and the media.[23] A comparable list compiled today would almost certainly include additional users and additional ways that health information is used.

These secondary uses of records are not without risk to the subjects of the records. In his classic study of health records, Professor Alan Westin observed that the disclosure of health information can have an enormous impact on people's lives—

> It affects decision on whether they are hired or fired; whether they can secure business licenses and life insurance; whether they are permitted to drive cars; whether they are placed under police surveillance or labelled a security risk; or even whether they can get nominated for and elected to political office.[24]

Rep. Nydia Velázquez testified about a personal experience involving the leaking of her health records during a political campaign. While the purpose of the leak was to affect the campaign, the personal effects on Rep. Velázquez and her family were harrowing. She noted that in some states, it is easier to obtain a person's medical history than it is to obtain the records of that person's video rentals.[25]

The consequences of improper disclosure of health information can be severe. But it is the routine disclosure and use of health information that may pose the greatest risk to the privacy interests of the average consumer. The growing computerization of health information is increasing both the supply of health data and the demand for that data. A recent report by the Institute of Medicine identifies many potential users of information maintained by health database organizations, a developing class of entities that collect and facilitate the sharing of health data on patients and providers.[26] Similarly, a report from the Office of Technology Assessment (OTA) about computerized medical information refers to the "tremendous outward flow of information generated in the health care relationship today" and to the "expanded use of medical records for nontreatment purposes." The report also suggests the possibility of a "proliferation of private sector computer databases and data exchanges without regulation, statutory guidance, or recourse for persons wronged by abuse of data."[27]

There is already a significant demand for health data about individuals for use in direct marketing. This is a category of users that

---

[23] American Medical Record Association, Confidentiality of Patient Health Information: A Position Statement of the American Medical Record Association 5–6 (1977), reprinted in 1979 House Hearings at 326–27.

[24] Alan F. Westin, "Computers, Health Records, and Citizen's Rights" 60 (U.S. Department of Commerce) (1976). A more recent review of privacy and health information reached the same conclusion. See Institute of Medicine, "Health Data in the Information Age: Use, Disclosure, and Privacy," chapter 4, pages 4–5 (1994) [hereinafter cited as "IOM Health Data Report"].

[25] H.R. 4077 Hearings (April 20, 1994).

[26] See generally IOM Health Data Report.

[27] Office of Technology Assessment, "Protecting Privacy in Computerized Medical Information" 44 (1993) [hereinafter cited as "OTA Medical Privacy Report"].

was not identified by the American Medical Records Association in 1977. Marketing and mailing list companies compile and sell lists of individuals with a variety of ailments. For example, one mailing list company maintains a database of 15 million individuals, including: 2.7 million hypertensives; 2.2 million hypercholesterolemics; 226,000 angina sufferers; 1 million diabetics; 3.5 million arthritics; 6 million allergy sufferers; 1 million heavy antacid users; 281,000 estrogen replacement patients; 459,000 gastritis sufferers; and 150,000 osteoporosis sufferers.[28]

This database also includes the names of Alzheimer's patients, individuals with bladder control problems, and Parkinson's disease sufferers.[29] The same firm merges the medical data with behavioral and demographic information from a lifestyle database.[30] Primary users of the data are reported to be pharmaceutical companies.[31] The patients, however, may not be the only target of marketing efforts. Sales to nonprofit groups wishing to target the families of sufferers are under consideration.[32] The Committee is not aware of any legal restrictions on the purchase and sale of personally identifiable health information from this database.

To develop the database, the company used answers from questionnaires sent to consumers.[33] According to Lorna Christie, Senior Vice President of the Direct Marketing Association, others use the ability to capture the names of callers to 800 telephone numbers as a way of identifying hay fever sufferers.[34] Other sources of personal health information cited by Christie include club memberships, pharmacies, and sign-up sheets in doctor's offices.[35] Super-

---

[28] Schultz, "Carlson, Metromail Offer Medical Data", DM News (June 21, 1993).

[29] Id.

[30] Id.

[31] Id.

[32] Id.

[33] For a description of how personal medical information is collected for use in direct marketing, see Erik Larson, "The Naked Consumer", 72–74 (1992). Larson explains how information about pregnant women and new mothers is collected and used for direct marketing. Id. at 79–97.

[34] Christie, "Health Data and the Private Sector" in "Health Records: Social Needs and Personal Privacy", 31 (1993) (conference proceedings). In another reported use of 800 numbers, a company offered a toll-free number to consumers (aimed primarily at older women) who wanted information about incontinence pads. The company then offered the list of names for sale, together with the caller's age, income, and other information. See Carnevale, "Caller ID Services Accused of Invading Individual's Privacy", Wall Street Journal at B2 (June 25, 1993). See also DM News at 2 (June 21, 1993).

[35] Christie, "Health Data and the Private Sector" in "Health Records: Social Needs and Personal Privacy", 30 (1993) (conference proceedings). It is unclear whether consumers who engage in any of these activities or disclosures are informed of the extent to which their personal information may be used. Whether these consumers are informed that the information can be added to mailing lists and sold commercially is also unclear. For a discussion of the use of identifiable information about consumers collected at supermarkets, see "Data Protection, Computers, and Changing Information Practices", Hearing before the Subcomm. on Government Information, Justice, and Agriculture, House Comm. on Government Operations, 101st Cong., 2d Sess. (1990). In one supermarket program, the notice of uses and disclosures states: "Since your purchases will be automatically recorded, this allows us to provide you with other special offers and information about items that may be of interest to you—both from our stores and from other carefully screened companies. If you do not wish to receive coupons, offers or other information, please check the box below." Id. at 119. The adequacy of these notices was identified by other witnesses as a critical question: "The critical question is, is the consent informed? Does the customer know in fact how the information is going to be used? As I said before, I don't think there is anything wrong with companies becoming more responsive to the needs of the customers. I do think there is something wrong when information is gathered and used in a way that the customer would likely object to if he or she know what was taking place." Id. at 121 (testimony of Marc Rotenberg, Director, Washington Office, Computer Professionals for Social Responsibility).

markets also may be a source of information about consumers.[36] Another example reported by Christie involved a blood bank that marketed lists of consumers who had blood tests. Christie cited the sale of data from a blood bank as an example of using and marketing health data inappropriately.[37] It is not clear whether any of these collection techniques included notice to consumers about the intended sale of data or offered consumers the ability to approve or veto the sale of their information.

Professor Paul Schwartz of the University of Arkansas Law School at Fayetteville testified about the use of health information by marketers:

> The protection for medical information is so weak in this country that marketing lists detailing the most sensitive information about citizens are for sale. Here is additional proof of the failure of current legal regulation. Johnson & Johnson has compiled a list for sale of five million elderly, incontinent American women. Another company has advertised lists containing the names of six million allergy sufferers, 700,000 people with bleeding gums, and 67,000 with epilepsy. Other citizens appear on a mailing list as suitable consumers of products intended for impotent middle-aged men.[38]

The OTA report found that other private sector repositories of patient information were being developed and implemented. One company provides interactive communications services to physicians in exchange for a modest fee and an agreement by the physician to watch certain promotional/educational materials. The physician maintains patient records on the computer system and allows the service provider to use aggregate clinical data for commercial purposes.[39] In another example cited by OTA, a private company collects identifiable records of prescription drug use and sells the database for use in marketing. It appears that patient identifiers are now stripped before sale, but this may not have always been true.[40] The Institute of Medicine report notes that the purchase of Medco Containment Services, a mail-order prescription firm, by Merck & Company, was based in part on the value of the information in its databases to influence physician prescribing practices.[41] Other similar mergers and acquisitions between drug manufacturers and prescription fulfillment firms are in process.

Whatever the source of the health information used in marketing, these examples illustrate that there is a demand for health data about identified individuals and that there are companies that will collect and sell data to fill that demand. Not all companies are willing to traffic in personal medical data, but it is apparent that

---

[36] Christie, "Health Data and the Private Sector" in "Health Records: Social Needs and Personal Privacy", 30 (1993) (conference proceedings). at 31. The sale of health-related information by retailers of non-prescription drugs and remedies is beyond the scope of the legislation. Trafficking in this type of personal health data (e.g., purchasers of over-the-counter allergy and hemorrhoid remedies) is not subject to any legislative or regulatory controls at this time. The propriety of trafficking in identifiable health-related information without the express consent of consumers after full disclosure of all uses and disclosures of the data is questionable.

[37] Id. at 31.

[38] H.R. 4077 Hearings (May 4, 1994) (footnotes omitted).

[39] OTA Medical Privacy Report at 33.

[40] Id. at 35.

[41] IOM Health Data Report at chapter 4, page 5.

some are. Powerful computers combine medical information with other demographic and personal data to enhance the value of the list being sold. One consequence is the creation of more detailed consumer profiles that combine data previously maintained in separate databases or by independent organizations. OTA notes that "the private sector has begun now to respond to a strong commercial incentive to aggregate medical information."[42] OTA also notes that businesses with access to identifiable information who are involved in selling aggregate patient data "operate under no regulatory guidelines regarding security measures, employee practices, or licensing requirements."[43]

The growing demand for and supply of health information for uses that are far removed from the health treatment and payment process make it imperative to establish a system of controls for identifiable health information that limits the unrestricted spread of that information. Existing legal and ethical rules governing patient data are inadequate to cope with modern public and private sector information practices. Even in those places where a physician operates under strict ethical or legal restrictions, data may lose its protection when the physician shares it in the ordinary course of business with a computer service company, an insurance claims processor, or an office management company. It is no longer sufficient to have rules that apply only to some persons who have access to identifiable patient information. To be effective and meaningful, rules must apply whenever patient data moves from the treatment and payment system to other places. The expanding use of identifiable patient data in the unregulated consumer marketing arena is also a serious concern and one that may require additional scrutiny in the near future.

Abuse of health information

Rules for protecting health information cannot be limited to evaluating the propriety of uses by those who are lawfully in possession of the data. Evidence developed by the Committee in 1979 suggests that surreptitious trafficking in health information may be common and nationwide. Strong criminal penalties are needed to deter and punish those who may be tempted to use health information improperly.

The best documented American example of abuse of health records comes from Denver, Colorado. Beginning in 1975, the Denver District Attorney and a grand jury began an investigation of the theft of health records. They found that for over twenty-five years, a private investigative reporting company known as Factual Services Bureau, Inc., engaged in a nationwide business of obtaining health information without the consent of the patient.

The company's investigators typically posed as doctors and sought medical information by telephone from public and private hospitals, clinics, and doctors' offices, including psychiatrists' offices. The company paid hospital employees to smuggle out health records. Another technique involved the use of false pretenses through mail solicitations. The company was successful in obtain-

[42] OTA Medical Privacy Report at 30.
[43] Id. at 31.

ing health records most of the time, and it even advertised its ability to acquire health records.

The customers of Factual Services Bureau included over one hundred of the most prominent insurance companies in the country. In a search of the Denver office of Factual Services Bureau, the District Attorney found almost two thousand reports to insurance companies. These reports frequently included detailed medical information about individuals that was obtained without the knowledge or consent of the individuals. No insurance company ever reported this questionable activity to law enforcement authorities.

In June 1976, the Denver grand jury issued a special report to the Privacy Protection Study Commission. The report stated that trafficking in patient records was a nationwide problem: "From the evidence, it is clear that the problem with respect to the privacy of medical records in this jurisdiction exists in many cities and jurisdictions across the nation." [44]

In testimony submitted during 1979 hearings, Denver District Attorney Dale Tooley said: "I find it difficult to believe that there are not or have not been similar enterprises engaged in this profitable, surreptitious business." [45]

Additional direct evidence that this type of trafficking in health information is widespread in this country is hard to find because there have been no investigations focusing on health records in recent years. However, evidence of illegal trafficking in other types of personal information is easy to find. For example, the General Accounting Office recently reported on misuse of criminal history information maintained by the National Crime Information Center (NCIC).[46] GAO found that the NCIC system was vulnerable to misuse, that misuse occurred throughout the NCIC system, and that some misuse was intentional. A limited review by GAO found sixty-two examples involving misuse, including these two:

> The California Department of Justice received a complaint from a person who suspected his employer of obtaining a copy of his criminal record from the NCIC's [Interstate Identification Index] file. A search of the state system's audit trail showed that the record had been accessed by a law enforcement agency in the eastern United States. Apparently, the employer had hired a private investigator, located in the eastern United States, to conduct background searches on prospective employees. The complainant's criminal history record was allegedly sold to the private investigator by an officer in a law enforcement agency.[47]
>
> A private investigator paid several city employees to conduct NCIC record searches. During the service of a search warrant at the investigator's office in an unrelated fraud matter, state investigators discovered records indicating that payments had been made for NCIC records and notified the Colorado Bureau of Investigation. The ensuing in-

[44] PPSC Report at 285.
[45] 1979 House Hearings at 1066.
[46] General Accounting Office, "National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information" (GAO/T–GGD–93–41) (1993).
[47] Id. at 24.

quiry, with the cooperation of the district attorney, resulted in the indictment of several individuals.[48]

These examples are similar to the illegal buying and selling of personal information uncovered by the Denver grand jury.

Other types of sensitive personal records are also routinely bought and sold. One recent investigation found a nationwide network of information brokers who obtained information from the NCIC, the National Law Enforcement Telecommunications System, the Military Personnel Records Center, the Social Security Administration, the telephone companies, and others. The information was provided in exchange for money by insiders who knew that it was against the law and policy of their agency or company.[49] There is even evidence of open solicitation through newspaper advertising of the ability to obtain records that are legally protected against improper disclosure.[50]

Evidence supporting the notion that there is routine illegal trafficking in health information also comes from Canada. In 1979, Mr. Justice Horace Krever, Commissioner of the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, Canada, testified before the Subcommittee on Government Information and Individual Rights.[51] The Royal Commission of Inquiry had its origins in press stories about abuse of confidential health information. Mr. Justice Krever testified that at the time the inquiry began, no one had any clear idea of the extent of the violation of confidentiality or that many violations were in the private casualty insurance sector.[52]

The Royal Commission found that the acquisition of health information by private investigators without patient consent and through false pretenses was widespread. During a 14-month period, the Royal Commission heard from over 500 witnesses, including private investigative firms, insurance companies, hospitals, and others. For the years 1976 and 1977, the Royal Commission found that there were hundreds of attempts made in Ontario to acquire health information from hospitals and doctors; well over half of the attempts were successful. Several investigative firms went out of business as a result of the Royal Commission's work.[53]

So many insurance companies were found to have been using health information obtained under false pretenses that the Insurance Bureau of Canada made a general admission to the Royal Commission that its members had gathered medical information through various sources without the authorization of the patient. Many members of the Insurance Bureau of Canada are subsidiaries of American insurance companies. Some investigative agencies that obtained information under false pretenses are also subsidiaries of American companies.[54]

---

[48] Id. at 26.

[49] See "Sale of Criminal History Records," Hearing before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 102d Cong., 2d Sess. 7 (1992) (Serial No. 87) (testimony of David F. Nemecek, Federal Bureau of Investigation).

[50] Id.

[51] 1979 House Hearings at 499–553.

[52] Id. at 508.

[53] Id. at 508–536.

[54] Id. at 538–41, 549–51.

Mr. Justice Krever testified that he was "very much surprised"[55] by the abuses of health information that the Royal Commission uncovered. He also testified that he suspected that the practices occurred not only in Ontario but throughout all of North America.[56]

Because of the similarities between the Canadian and American casualty insurance industry and the private investigation industry, this Committee inferred in a 1980 report that the same techniques for acquiring health information that were used in Canada were also used in the United States. The techniques used by the Factual Services Bureau were identical to those common in Canada. All of the people involved in the Denver and Canadian investigations have stated their view that the practices were common throughout the United States.[57]

A recent book on privacy and computers by Jeffrey Rothfeder included this description of the collection of personal information in America—

> [I]nformation about every move we make—buying a car or a home, applying for a loan, taking out insurance, purchasing potato chips, requesting a government grant, getting turned down for credit, going to work, seeing a doctor—is fed into dozens and dozens of separate databases owned by the credit bureaus, the government, banks, insurance companies, direct-marketing companies, and other interested corporations. And from these databases it's broadcast to thousands and thousands of regional databanks as well as to numerous information resellers across the country. Then the data is shipped to millions of computers on corporate desktops or in people's homes throughout the country.[58]

The legal use of personal information is disturbing enough. Rothfeder also documented the underground or illegal use of personal data:

> The information underground taps into legitimate data sellers—they're highly active customers of the credit bureaus, motor vehicle agencies, and real estate databanks, for instance—and also buys data from illicit suppliers, such as bank and medical networks.[59]

The Institute of Medicine (IOM) also expressed alarm about the acquisition and use of medical information through illegal or unethical means.[60]

Based on past investigations and on more recent evidence of widespread, legal and illegal buying and selling of personal information protected by law, the Committee sees no reason to change the 1980 conclusion that there is routine trafficking in health records in the United States. If anything, organized trafficking in personal records, both legal and illegal, may have increased in the

---

[55] Id. at 543.
[56] Id. at 508, 511.
[57] See Comm. on Government Operations, H.R. Rep. No. 96–832, Part I, 96th Cong., 2d Sess. 27 (1980) (report to accompany H.R. 5935).
[58] Jeffrey Rothfeder, "Privacy For Sale" 22–3 (1992).
[59] Id. at 64.
[60] IOM Health Data Report at chapter 4, page 18–19.

last fifteen years. Clear rules and strong penalties are needed in order to prevent the dozens of secondary users from responding to commercial and other pressures to make greater use—illegal or otherwise—of health information in their possession.

Inadequate legal and ethical guidance

Federal legislation to establish fair information practices standards for health information is also needed because existing confidentiality rules are inadequate. This has been a consistent finding of studies in recent years.

The Office of Technology Assessment recently completed a review focusing on health privacy and computers. OTA noted that privacy of health care information has been primarily protected through a patchwork system of ethical obligations and legal rights. OTA found, however, that this system is inadequate.

> *The present system of protection for health care information offers a patchwork of codes; State laws of varying scope; and Federal laws applicable to only limited kinds of information, or information maintained specifically by the Federal Government.*[61]

OTA reached this blunt conclusion:

> *The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment.*[62]

The Institute of Medicine review of health privacy found three weaknesses in legal confidentiality protections for health records. First, the degree to which confidentiality is required varies according to the holder of the information and the type of information held. Second, legal obligations often vary widely within a single state and from state to state. Third, current laws offer patients little real protection against redisclosure. The IOM found that "[r]edisclosure practices represent a yawning gap in confidentiality protection."[63]

Another commentator has written about the failure of traditional legal and ethical confidentiality principles to help physicians in resolving conflicts over the use of health information:

> Now that medical records are a more reliable and comprehensive source of information about patients, requests for the disclosure of identifiable medical information are made more frequently and by a wider variety of institutions than ever before. As patient information is increasingly sought for purposes not directly related to medical treatment, conflicts over the use of medical records become more acute. Because the complexity of the physician's responsibility has not been fully recognized, however, traditional legal and ethical confidentiality principles provide little assistance in resolving these conflicts.[64]

---

[61] OTA Medical Privacy Report at 12–13 (original emphasis).
[62] Id. (original emphasis).
[63] IOM Health Data Report at chapter 4, page 12.
[64] Gellman at 255.

The Workgroup for Electronic Data Interchange (WEDI), an industry-led group established to examine the potential for uniform electronic billing, reached a similar conclusion:

> Myriad laws and regulations require providers to maintain health information in a confidential manner. These legal parameters are difficult to catalog because confidentiality has historically been addressed at the state level, with each state crafting its own unique approach. The state rules are superimposed on a federal regulatory framework. The result: a morass of erratic law, both statutory and judicial, defining the confidentiality of health information.[65]

Several witnesses at an initial hearing held by the Subcommittee on Information, Justice, Transportation, and Agriculture offered similar views. Robert Johnson, representing the American Hospital Association, testified about the shortcomings of existing laws and regulations. He also said that administrative efficiencies would result from uniform laws governing patient information:

> As we begin to build a nationwide information infrastructure, we must examine the currently inconsistent laws and regulations which govern the exchange of patient information. Many state and federal laws create obstacles to the legitimate sharing of health information that could yield better patient care, administrative savings, and more efficient patient management. For example, some states prohibit the use of computerized record systems by requiring that orders be written in ink, often referred to as the "quill pen" laws or by restricting the permissible health record storage media to the original paper or microfilm.
>
> Moreover, payers and providers that operate in more than one state are required to comply with a multitude of different rules, which adds to administrative inefficiency. The obligation of complying with individual—often inconsistent—state laws and regulations is overly burdensome and costly.
>
> Despite this plethora of state laws, most of which include some form of confidentiality protection, identifiable health care information still remains vulnerable to unauthorized disclosures. Furthermore, many state laws do not address key issues, like the patient's right to see, copy, and correct his or her own records, and the obligations of anyone who comes in contact with individually identifiable health care information—including but not limited to payers, providers, processing vendors, storage vendors and utilization review organizations—to protect confidentiality. As a result, the current system promotes confusion over con-

[65] Workgroup for Electronic Data Interchange, "Report to Secretary of U.S. Department of Health and Human Services" at Appendix 4, page 5 (1992).

fidentiality rights with varying requirements from state to state.[66]

Kathleen Frawley, representing the American Health Information Management Association, testified about the need for uniformity and the failure of the states to enact uniform health information legislation:

> Many states have enacted legislation modeled after the [Federal] Privacy Act. It has been recognized, however, that there is a need for more uniformity among the 50 states. In recent years, the National Conference of Commissioners on Uniform State Laws developed the Uniform Health Care Information Act in an attempt to stimulate uniformity among states on health care information management issues. Presently, only two states, Montana and Washington, have enacted this model legislation. Clearly, efforts must be directed toward developing national standards to support the evolution of the computer-based patient record.[67]

Janlori Goldman, Director of the American Civil Liberties Union's Privacy and Technology Project testified about the need for a uniform federal law and about how the existing patchwork approach can hamper health reform:

> The outcome of this piecemeal, state by state, approach to protecting the privacy and security of health care information will be contradictory and detrimental to both the individuals and the goals of health care reform. Relegating the protection of health care information to the states' different guidelines, policies and laws leaves individuals subject to wavering degrees of privacy protection depending upon where they receive their health care. In some instances, this means that individuals traveling across county or state lines to receive necessary medical treatment may lose their ability to control how their health care information is used.
>
> Such a patchwork approach to health information privacy will hamper a national system. The various states and localities with rules governing the use of health care information may even be prevented from sharing health care information contained in their systems with neighboring states that insufficiently protect privacy. Thus, there is a clear need for a uniform federal law that will protect individuals' health care information and provide guidance to the states and localities engaged in health care reform.[68]

The OTA report suggests that the growing use of computers is putting even more pressure on the existing system of piecemeal protection and that existing patient protections will become increasingly ineffective:

---

[66] "Health Reform, Health Records, Computers and Confidentiality", Hearing before the Information, Justice, Transportation, and Agriculture Subcomm. of the House Comm. on Government Operations, 103rd Cong., 1st Sess. (1993) (to be printed).

[67] Id.

[68] Id.

> As a result of the linkage of computers, patient information will no longer be maintained, be accessed, or even necessarily originate with a single institution, but will instead travel among a myriad of facilities. As a result, *the limited protection to privacy of health care information now in place will be further strained. Existing models for data protection, which place responsibility for privacy on individual institutions, will no longer be workable for new systems of computer linkage and exchange of information across high-performance, interactive networks. New approaches to data protection must track the flow of the data itself.*[69]

Finally, the Privacy Protection Study Commission stated that the confidentiality of the doctor-patient relationship cannot be restored simply by placing limitations on government access to health records. The 1977 report of the Commission explains why broader legislation is needed:

> If a record keeper has the discretion to disclose voluntarily, it will be hard for record keepers, particularly in heavily regulated sectors such as banking, to resist pressures for "voluntary" compliance with government requests for information. Voluntary disclosure of information on individuals held by third parties must be limited if limitations on compelled disclosure are to mean anything.[70]

The Committee concludes with a great deal of confidence that the time has come for a federal law establishing uniform fair information practices for health information.

Privacy and fair information practices

In 1980, the Committee on Government Operations reported a bill titled "Federal Privacy of Medical Information Act." The 1994 legislation is titled "Fair Health Information Practices." While there are many similarities in purpose, language, and effect between these bills, the change in title bears some significance.

The first general code of fair information practices was proposed by an Advisory Committee at the Department of Health, Education, & Welfare in 1973.[71] The notion of fair information practices has grown in importance, forming the basis for a common set of principles for privacy (or data protection[72]) laws around the world. One formulation of a code of fair information practices is:

---

[69] OTA Medical Privacy Report at 9–10 (original emphasis).

[70] PPSC Report at 351.

[71] Department of Health, Education, & Welfare, "Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens" (1973) [hereinafter cited as "HEW Report"]. For a discussion of the importance of the work of the Advisory Committee, see Gellman, "Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," VI Software Law Journal 199, 209–212 (1993). There is evidence of the simultaneous development of almost the identical concept in Britain by the Younger Commission. See Colin J. Bennett, "Regulating Privacy: Data Protection and Public Policy in Europe and the United States" 99 (1992).

[72] "Data protection" is a more precise way of referring to privacy values that arise in connection with the collection, use, and dissemination of personal information. See David Flaherty, "Protecting Privacy in Surveillance Societies" 11 (1989) ("Under the broad rubric of ensuring privacy, the primary purpose of data protection is the control of surveillance of the public, whether this monitoring uses the data bases of governments or of the private sector.") [hereinafter cited as "Flaherty." See also 137 Congressional Record H 755 (Jan. 29, 1991) (Statement of Rep. Bob Wise upon the introduction of the Data Protection Act of 1991, H.R. 685, 102nd Cong.).

(1) The Principle of Openness, which provides that the existence of record-keeping systems and databanks containing data about individuals be publicly known, along with a description of main purpose and uses of the data.

(2) The Principle of Individual Participation, which provides that each individual should have a right to see any data about himself or herself and to correct or remove any data that is not timely, accurate relevant, or complete.

(3) The Principle of Collection Limitation, which provides that there should be limits to the collection of personal data, that data should be collected by lawful and fair means, and that data should be collected, where appropriate, with the knowledge or consent of the subject.

(4) The Principle of Data Quality, which provides that personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete, and timely.

(5) The Principle of Use Limitation, which provides that there must be limits to the internal uses of personal data and that the data should be used only for the purposes specified at the time of collection.

(6) The Principle of Disclosure Limitation, which provides that personal data should not be communicated externally without the consent of the data subject or other legal authority.

(7) The Principle of Security, which provides that personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure. Sufficient resources should be available to offer reasonable assurances that security goals will be accomplished.

(8) The Principle of Accountability, which provides that record keepers should be accountable for complying with fair information practices.[73]

There are several reasons why a code of fair information practices bill has been proposed rather than a privacy bill. First, privacy is a broad and sometimes vague concept, with many different elements depending on the context.[74] On the other hand, fair information practices are more specific and more narrowly focused on the protection and appropriate use of personal information. Protection of identifiable health information is the goal of the legislation.

Second, it is apparent to anyone who views the modern health care system that health records are not strictly "private." There are simply too many governmental agencies and other institutions that use identifiable health records to accomplish important objectives, including protection of public health, cost containment, health research, and fraud prevention. While it may be unfortunate, it is

---

[73] This statement of fair information practices is derived from many sources, including HEW Report; Organization for Economic Cooperation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1981); Council of Europe, "Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data" (1981). The latter two documents are reprinted in "Data Protection, Computers, and Changing Information Practices," hearing before the Subcomm. on Government Information, Justice, and Agriculture, House Comm. on Government Operations, 101st Cong., 2d Sess. (1990). See also "OTA Medical Privacy Report" at 77–9.

[74] There is no universally agreed upon definition for "privacy" and "confidentiality." For one view of these terms, see "IOM Health Data Report" at chapter 4, pages 6–13.

true that much health information is no longer shared only between doctor and patient. In the last decade of the twentieth century, it is simply not possible to propose legislation that can promise that health information will be absolutely private. What can and must be guaranteed to each patient is that his or her health information will be used fairly and disclosed only when necessary. Fair information practices for health information can be provided even though absolute privacy cannot.

Findings and purposes

Because of the restructuring that was necessary when the Fair Health Information Practices Act (H.R. 4077) was added as the Fair Health Information Practices Part of H.R. 3600, the findings and purposes were omitted. They remain relevant to the legislation and are reproduced here.

Findings.—The Congress finds as follows:

(1) The right to privacy is a personal and fundamental right protected by the Constitution of the United States.

(2) The improper use or disclosure of individually identifiable health information about an individual may cause significant harm to the interests of the individual in privacy and health care, and may unfairly affect the ability of the individual to obtain employment, education, insurance, credit, and other necessities.

(3) Current legal protections for health information vary from State to State and are inadequate to meet the need for fair information practices standards.

(4) The use, maintenance, and disclosure of health information affects interstate commerce because of the movement of individuals, health care providers, and health information across State lines; access to and transfer of health information from automated data banks and interstate telecommunications and computer networks; the exchange of health information through the mail; and the provision of and payment for health care through interstate means.

(5) Uniform rules governing the use, maintenance, and disclosure of health information are an essential part of health care reform, are necessary to support the computerization of health information, and can reduce the cost of providing health services by making the necessary transfer of health information more efficient.

(6) There is a compelling need for uniform Federal law, rules, and procedures governing the use, maintenance, and disclosure of health information.

(7) Individuals need access to their health information as a matter of fairness, to enable the individual to make informed decisions about health care, and to correct inaccurate or incomplete information.

(b) Purposes.—The purposes of this Act are as follows:

(1) To define the rights of an individual with respect to health information about the individual that is created or maintained as part of the health care treatment and payment process.

(2) To define the rights and responsibilities of a person who creates or maintains individually identifiable health information that originates or is used in the health treatment or payment process.

(3) To establish effective mechanisms to enforce the rights and responsibilities defined in this Act.

Hearings on Fair Health Information Practices

On November 4, 1993 the Subcommittee on Information, Justice, Transportation, and Agriculture held a public hearing on Health Reform, Health Records, Computers and Confidentiality. The witnesses at this hearing were: Paula J. Bruening, Project Director and Legal Analyst, Office of Technology Assessment; Robert Johnson, American Hospital Association, Vice President and General Counsel, Catholic Healthcare West; Dr. Donald Lewers, Board of Trustees, American Medical Association; Janlori Goldman, Director, Privacy and Technology Project, American Civil Liberties Union; Kathleen Frawley, Director, Washington, D.C. Office, American Health Information Management Association; Dennis Drislane, President, Health Care Division, EDS.

On April 20, 1994 the Subcommittee held a public hearing on the Fair Health Information Practices Act of 1994 (H.R. 4077). The witnesses at this hearing were: Representative Nydia Velázquez (D–NY); Nan D. Hunter, Deputy General Counsel, Department of Health and Human Services; Dr. Alan Westin, Professor of Public Law and Government, Columbia University; John Baker, Senior Vice President, Equifax, Inc.

On May 4, 1994 the Subcommittee held a public hearing on the Fair Health Information Practices Act of 1994 (H.R. 4077). The witnesses at this hearing were: Dr. Donald Lewers, Board of Trustees, American Medical Association; Frederic Entin, Senior Vice President and General Counsel, American Hospital Association; Joel E. Gimpel, Associate General Counsel, Blue Cross and Blue Shield Association, Workgroup on Electronic Data Interchange; Kathleen Frawley, Director, Washington, D.C. Office, American Health Information Management Association; Dr. Richard Barker, President, Healthcare Industries, IBM; Dr. Martin Sepulveda, Director, Occupational Health Services, IBM; Robert S. Bolan, Chairman, Medic Alert Foundation International; Professor Paul Schwartz, University of Arkansas (Fayetteville) Law School.

On May 5, 1994 the Subcommittee held a public hearing on the Fair Health Information Practices Act of 1994 (H.R. 4077). The witnesses at this hearing were: Representative Thomas C. Sawyer (D–OH), Chairman, Subcommittee on Census, Statistics, and Postal Personnel; Aimee R. Berenson, Legislative Counsel, AIDS Action Counsel; Susan Jacobs, Staff Attorney, Legal Action Center; Janlori Goldman, Director, Privacy and Technology Project, American Civil Liberties Union.

Committee Consideration of Fair Health Information Practices

On July 27, 1994, the Subcommittee on Information, Justice, Transportation, and Agriculture, a quorum being present, approved

by voice vote an amendment offered by Subcommittee Chairman Condit.

On July 27, 1994, the Committee on Government Operations, a quorum being present, approved by voice vote the amendment as reported by the Subcommittee, with an additional amendment offered by Mr. Towns. That amendment provided rules for the disposition of health records for providers and others who have gone out of business. The Committee ordered the Subcommittee amendment, as amended, reported.

In addition, the Committee approved by voice vote an amendment offered by Mr. Thomas that amended part 1 of subtitle B of title V. The amendment encourages the development of a distributed electronic data network for purposes of establishing uniform standards for the electronic transmission of financial, administrative, and clinical data.

It requires the Secretary of Health and Human Services to establish standards for automating health care data. To the maximum extent possible, the Secretary shall incorporate standards that are currently in use or developed by private standard-setting organizations, including the American National Standards Institute and the Healthcare Informatics Standards Planning Panel. This requirement is consistent with Administration policy (e.g., OMB Circular A–119).

The amendment repeals state "Quill Pen" laws, which require that health records be maintained in written form. In addition, the amendment authorizes the Secretary of Health and Human Services to support demonstration projects in rural and urban areas for the purpose of accelerating progress in the area of electronically integrated, community-based clinical information systems. The funds received under this section may be used to enhance existing telecommunications and information systems.

Section-by-Section Analysis and Discussion of Fair Health Information Practices

SECTION 5120. DEFINITIONS.

Section 5120 contains definitions relating to protected health information, health information trustees, and other definitions.

"Protected health information" is one of the key terms. The basic requirements of the Fair Health Information Practices part apply to protected health information. There are essentially three requirements that must be met for information to qualify as protected health information. First, the information must be created or received by a health care provider, health benefit plan, health oversight agency, or health information service organization in a state. The definition does not cover health information wherever situated. Only information created by or used in the treatment or payment process qualifies.

Second, information only qualifies if it relates in any way to the past, present, or future physical or mental condition or functional status of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual. Any information created or received incident to the provision of health care or incident to payment for health care is covered. If a

physician or health insurer acquires the name, identification number, employment status, address, financial data, family size, education, employment history, or any other type of demographic information about a patient incident to the provision of or payment for health care, that information qualifies as protected health information. A provider or insurer cannot divide a patient's record into health and non-health matters and conclude that the non-health portion does not qualify as protected health information. Even the basic fact that John Doe is a patient of Dr. Jane Smith is protected health information. Any information conveyed during treatment or consultation or related in any way at all to health care or health status is protected health information. Information that is otherwise public or seemingly not sensitive is protected health information when it becomes part of a provider's or insurer's record.

This result is crucial because the health care system may lead to the routine collection of large amounts of personal information relating directly to health care, health status, life style, and enrollment eligibility. Eventually, much of the information in a health record will be computerized. If this massive databank—centralized, networked, or otherwise linked or linkable—is used for unrelated administrative, law enforcement, or other purposes, then the detrimental effects on individual privacy and on the relationship between physician and patient will be significantly compounded. To the greatest extent practicable, data collected and maintained for use in the health care treatment and payment system should not be available for other purposes.

Genetic information is an especially sensitive and increasingly important component of protected health information. The role of genetics in health care is expanding as researchers discover the genes associated with many health conditions. This knowledge will improve the ability to diagnose existing disorders and predict late-onset disorders, to determine susceptibility to disorders caused by conditions during one's lifetime, and to treat or prevent these disorders. Increasingly, genetic information about individuals will be learned before they are born. This expanded information about individuals will also pertain to their offspring and other blood relatives. The sensitivity of genetic information cannot be overestimated. In addition to assisting diagnosis and treatment, genetic information can also be used to discriminate, to stigmatize, and to reduce individuals' control over their lives.

Information about an individual's genetic characteristics that is created or received by a health information trustee in connection with health care or payment for health care qualifies as protected health information. It makes no difference what the particular genetic characteristic may indicate. Information about physical features, personality characteristics, likelihood for contracting specific diseases, personality or other traits likely shared by children or other relatives, and any other genetic markers qualify. Even if there is no immediate known relationship between a genetic characteristic and an individual's health, information derived from genetic testing falls within the definition of protected health information.

Genetic information can identify an individual in two distinct ways: (1) as with other kinds of medical information, genetic infor-

mation can identify an individual by including the individual's name or other (nongenetic) information about the individual, such as the social security or other identification number, or vital statistics about the individual; or (2) genetic information can be used for forensic purposes to establish a blood relationship between individuals, the identity of a dead person, or the likelihood that a biological sample recovered at a crime scene came from a particular individual, by comparing biological samples at the molecular level. For the purposes of this part, identification is used in the first of these meanings, that is, genetic information that identifies or can readily be used to identify an individual means genetic information about an individual that includes the individual's name or other (nongenetic) identifying information.

The third requirement that must be met for health information to qualify as protected health information is that an individual who is a subject of the information must be identifiable. For example, information is clearly identifiable if it includes a name, social security number or other generally known or readily available identification number, or photograph. Protected health information will not usually include data that is completely devoid of all individually identifiable information, data about physicians or hospitals, or aggregate data compiled for statistical use.

Information is identifiable if there is a reasonable basis to believe that the information can be used to identify an individual. In making an assessment of reasonableness under the Part, it may be necessary at times to make a judgment based on other information that is available to a recipient. For example, most people cannot identify an individual from a fingerprint. A law enforcement agency, however, must be presumed to have that capability. There would, therefore, be a reasonable basis to believe that disclosure of a record with a fingerprint to a law enforcement agency could be used readily to identify an individual. The disclosure of the same record to a private health researcher would not meet the test.[75]

When information is published, however, it must be assumed that the data may be seen by people with all reasonably known identification capabilities. This standard is not being adopted to change the current policies for publication of research articles. A review of current literature suggests that a test of reasonableness is already generally in use.

The release of non-unique data also may allow the identification of particular individuals. For example, the occupational description "professional athlete" is a non-unique identifier as is the diagnosis "amyotrophic lateral sclerosis". There are many individuals who are or have been professional athletes and some individuals who have suffered from amyotrophic lateral sclerosis. Yet many people could tell that a description of a professional athlete with amyotrophic lateral sclerosis referred to Lou Gehrig.

Lou Gehrig can be identified from the above description because of the publicity that surrounded his illness. An equally specific de-

[75] A change in technology or in the availability of technology would make a difference in a determination of what is reasonable. The ability to identify specific individuals from hair, blood, or other physical samples must be considered. If databases of fingerprints or hair characteristics or other personal data are maintained and become available to potential recipients, then this must also be considered.

scription in another case—a bus driver with cancer—would be truly non-identifiable. Even if the bus driver were identified as a resident of New York City, the information would likely remain non-identifiable. But if the bus driver were from a named small town, a different conclusion might result.

No single rule can define what constitutes readily identifiable data. The law uses a standard of "reasonable basis to believe". When assessing the reasonable likelihood of identification, trustees who disclose any information about a patient must consider all of the circumstances of the disclosure, including the specific knowledge and capabilities of any reasonably likely recipients. In the case of genetic information, extra consideration to the issue of identification may be appropriate because the comparison of genetic information about different individuals may lead to the identification of one or more of those individuals.

The remote chance that somebody might possibly be able to identify a patient from a general description does not meet the reasonable basis to believe standard. But the burden of justifying the disclosure of any information about an individual falls on the trustee making the disclosure. No extensive factual inquiry is necessary before making a disclosure, but doubts should always be resolved in favor of non-disclosure.[76] Overall, choices about what can be disclosed will be aided by the considerable body of work done in this area by federal statistical agencies.[77]

There is no requirement in the definition of "protected health information" that there must first be a confidential physician-patient relationship. Sensitive health information is routinely collected, created, or used by people who are not health care providers but who are nevertheless engaged in the provision of or payment for health care. From the patient's perspective, the information is no less sensitive or less deserving of protection as a result. In some present or future circumstances, health information may be even provided to and advice may be offered by a computer. The legislation takes the position that the patient's interest in confidentiality is the same in all of these situations. Once patient specific informa-

---

[76] One difficult circumstance may arise when information on specific patient encounters is disclosed with identifiers removed. Normally, data of this type will not be considered to be identifiable. But when information on identified patients has been independently placed in the public domain, it may be possible to associate the name of a public figure with the non-identifiable release. For example, movie star John Doe enters a hospital for surgery. Basic information about the type of surgery and location of the treatment is released with the consent of Mr. Doe. In addition, Mr. Doe's age may be publicly available from a variety of sources, including possibly state motor vehicle records. Knowing Mr. Doe's age and the nature and location of the treatment he received may allow an enterprising person to identify Mr. Doe's record from a computer tape containing thousands of patient encounters. The number of 50 year old white males receiving heart transplants at the Hospital of the University of Pennsylvania on January 11, 1994 is likely to be very small. In this circumstance where the patient has placed into the public domain some information that would enable otherwise non-identifiable data to be associated with that patient, the patient must bear the risk of identification. Extraordinary or impractical measures to remove or further anonymize routine patient encounter data are not required. Nevertheless, the release of fully anonymized patient encounter data may need to be regulated in order to limit the ability of even casual observers to link these records with individuals.

[77] See, e.g., Committee on National Statistics, "Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics" (1993) (National Research Council). The Panel on Confidentiality and Data Access of the Committee on National Statistics recommended continued government work on this issue. Id. at 155–157. The Panel noted that zero-risk requirements for disclosure of statistical records were unrealistic and recommended a standard that calls for a "reasonably low risk of disclosure of individually identifiable data." Id. at 137. See also Office of Management and Budget, "Report on Statistical Disclosure Limitation Methodology" (1994) (Statistical Policy Office).

tion is generated by or becomes part of the health care treatment or payment process, it becomes protected health information, regardless of the existence of a formal doctor-patient relationship at the time of creation or collection.

The term "health information trustee" identifies those who are in possession of protected health information and who have responsibilities under the Part.[78] This new term has been used to avoid traditional and more troublesome terms like "owner and record keeper." The idea of ownership of personal information maintained by third party record keepers is not particularly useful in today's complex world.[79] Any suggestion that one person in possession of personal information about another individual has complete dominion over or exclusive rights to the information is inaccurate, misleading, and unhelpful to any fair analysis of the rights and obligations of all of the interested parties.[80] This is likely to be an area in which new legal and policy principles are developed in the near future and extended to other types of records about individuals.

The Fair Health Information Practices Part makes it clear that both the trustee of protected health information and the subject of the information have rights and responsibilities with respect to data about the subject. The term "trustee" is not intended to be interpreted in the strict legal sense of one to whom property is legally committed to be administered for the benefit of another. Since both the trustee and the subject have rights with respect to the data, the term trustee should be read in its general sense as one to whom something is entrusted. A comparable term might be custodian in the sense of one who is entrusted with guarding and keeping records.

The implication that protected health information maintained by a trustee is sensitive and valuable is intentional, as is the implication that the trustee has a responsibility to look after the interests of others. But the duties and responsibilities of trustees are only those specified in the Part. The Committee cautions against any reading of the term "trustee" to imply any duties, responsibilities,

---

[78] Employers are not covered under the definition in their role as employers. An employer will nevertheless qualify as a health information trustee providing health care (i.e., first aid) or by processing claims for payment. A person carrying out either activity becomes a health information trustee with respect to that function and is subject to the applicable provisions of the Part. This includes, most notably in this context, the general limits on use and disclosure in section 5131. A trustee may only use or disclose protected health information for an authorized purpose. General use of protected health information by an employer for activities unrelated to the purpose for which the information was collected in prohibited. Thus, use of treatment records to make promotion decisions is a violation. Other laws, such as the Americans With Disabilities Act, may prohibit discriminatory or other use of the information as well. See also, Frawley & Waller, "Building a Chinese Wall: Protecting Employee Health Care Data," 2 DataLaw Report 1 (July 1994).

[79] See generally Branscomb, "Who Owns Information?" (1994).

[80] The Supreme Court's decision in *U.S.* v. *Miller,* 425 U.S. 435 (1976) is especially unhelpful. See the discussion of Miller elsewhere in this report. The point being made here is broader than the proper interpretation of the Fourth Amendment's restrictions on governmental action. Third parties maintain tremendous amounts of information on individuals. In the words of Professor David Flaherty, "[I]ndividuals in the Western world are increasingly subject to surveillance through the use of data bases in the public and private sectors * * *" *Flaherty* at 1. The notion that all of this personal information can be used or redisclosed by the third party record keepers without any regard for the interest of the subject of the information is old-fashioned, unreasonable, and not reflective of the large volume of information maintained or the consequences of the uses. The subject of the record has a clear interest in the information and that interest must be taken into account. This bill deliberately avoids any reliance on the "ownership" or "possession" approach to defining the rights of record subjects.

or rights not specifically enumerated in the Fair Health Information Practices Part.

The terms "carrier, health benefit plan," and "health benefit plan sponsor" are intended to cover those who provide any type of health insurance or conduct any type of health insurance enrollment function. The terms include those who provide self-insurance as well as those who provide insurance to others. The intent is to be as broadly encompassing as possible. Also included are insurance plans for accident, dental, vision, disability income, and long term care; Medicare supplemental health insurance; coverage issued as a supplement to liability insurance; liability insurance, including general liability insurance and automobile liability insurance; worker's compensation and similar insurance; automobile medical-payment insurance; coverage for specific diseases or illnesses; and hospital or fixed indemnity policies.

The term "health oversight agency" covers institutions that utilize protected health information in the course of carrying out activities that relate to the management or supervision of the health care system. Those engaged in licensing, accreditation, or certification of hospitals, physicians, or other health care providers are health oversight agencies. Also included are those federal or state agencies (and those acting on behalf of such agencies) who perform audits, assessments, evaluations, determinations, or investigations relating to the effectiveness of, compliance with, or applicability of, legal, fiscal, medical, or scientific standards or aspects of performance related to the delivery of or payment for health care.

For example, the Office of Inspector General (OIG) at the Department of Health and Human Services uses health records in its oversight and law enforcement roles with respect to programs conducted or funded by the Department of Health and Human Services. As a health oversight agency, in its conduct of these particular activities, it would have access to records held by health benefit plans, health care providers, other health oversight agencies, and health information service organizations, as necessary, under section 5133.

The OIG reviews patient records to validate diagnosis, treatment, and other patient specific medical information relative to federally financed health programs. The OIG also needs access to patient specific health records to assist in performance audits, inspections, and evaluations related to OIG oversight responsibilities for Peer Review Organizations (under title XI, part B of the Social Security Act), carriers and intermediaries in the Medicare program, and State Medicaid agencies. The Office also conducts audits and evaluations of federally operated health facilities and clinics and federally financed clinical research—including instances of contracted health services and supplies provided wholly or in part by the Federal government.

The inquiries are intended to detect a wide range of improper activities with respect to the health care system. They may result in criminal and civil prosecutions and administrative sanctions for conduct such as billing for services not provided; manipulation of diagnosis coding; misrepresentation of services rendered; provision of unnecessary or poor quality health care; and violation of patient dumping laws by hospitals and clinics.

The term "protected individual" is used to describe those individuals who are the subject of protected health information and who have rights under the Fair Health Information Practices Part. The term includes all living individuals and those who died within the last two years. Developing rules governing the records of deceased individuals is not a simple or obvious task.[81] Extending full protection to these records forever is expensive and unnecessary. Ending protection at the moment of death is equally unattractive. A balance between the two extreme alternatives is appropriate, and the two year period was selected as a reasonable middle ground. For all but a handful of individuals, any general interest in their medical condition will have been extinguished before the expiration of the two year period. At the end of this period, health records do not become public documents. Health information trustees may continue to apply their own appropriate confidentiality rules and procedures to the records and provide protections for records for a longer period.

The term "affiliated person" is used to cover a wide variety of people who are allowed to have access to protected health information by health information trustees. The purpose is to bring within the scope of the Part those persons who perform services on behalf of health information trustees but who are not trustees themselves or employees of trustees.

The concept of affiliated person is important because it allows a trustee to carry on its activities and operations as it sees fit while providing a method that will continue the protection of any protected health information that must be shared with others as a result of those activities and operations. Except where otherwise specifically provided, protected health information used or disclosed by a health information trustee remains subject to the protections of the Part whether the data is shared with another trustee or other party. The other party will normally be an affiliated person and will be subject to the Part's provision. This is consistent with the philosophy of the Fair Health Information Practices Part that protected health information usually remains covered no matter where it goes or who has access.[82]

By definition, an affiliated person must be someone who is not a health information trustee in its relationship with the trustee who is providing access to the protected health information. As a result, it is possible that the same person may be a health information trustee in one context and an affiliated person in another. This is best illustrated by an example.

Consider a health care provider, a health insurer, and a computer service firm. If the provider contracts with a computer serv-

[81] The traditional view is that privacy is a right of living individuals and one that does not extend beyond death. See American Civil Liberties Union Foundation, "Litigation under the Federal Open Government Laws" (1993) ("The weight of the authorities is that the personal privacy interests protected by Exemptions 6 and 7(C) [of the Freedom of Information Act] lapse upon the death of the individual." Id. at 129.). There is some case law that has held that surviving family members may have cognizable privacy interests in government records related to the death of a loved one. This is not actually the same interest as is recognized under the FOIA. For example, an individual has no standing to object to the release of embarrassing or shocking information by a living relative. The two year rule set out in section 5120 should be viewed as an exception to the traditional view of privacy. It is not intended to suggest the need to change the law in other areas.

[82] The exceptions to this policy include information disclosed to the patient, information disclosed to next of kin, and directory information that is disclosable to anyone.

ice firm to process protected health information on behalf of the provider, the computer service firm will be an affiliated person of the provider. When the provider (either directly or through the computer service firm) sends claims information to the health insurer for reimbursement, the health insurer is a health information trustee who receives information pursuant to the provision of the bill that authorizes disclosures for the purpose of providing for payment.

If the provider contracts with the insurer for computer services not directly related to the payment process, the insurer will be an affiliated person with respect to the provision of those services and with respect to the associated data disclosure. The insurer will remain a health information trustee with respect to its payment relationship to the provider.

This is not as complex or as unusual as it may appear at first glance. For example, a physician may be a health care provider with respect to one individual, a researcher with respect to another, an administrator with respect to other patients, and the next of kin of another individual. Similarly, a telephone company may have different relationships with other telephone companies. In one context, the company may be a regular customer of a second telephone company. In another context, the relationship may be that of an inter-exchange carrier. In each relationship, the rights and obligations are different. Correspondingly, a hospital may be an employer of an individual in one context and a health care provider in another.

An affiliated person also must be a contractor, subcontractor, associate, or subsidiary of a health information trustee and must, pursuant to an agreement or other relationship with the trustee, receive, create, use, maintain, or transmit protected health information. A person does not become an affiliated person simply by virtue of any type of contractual relationship with a trustee. For example, a person hired to paint the walls of a hospital does not become an affiliated person unless some type of access to protected health information is involved. Thus, a painter of a public area in a hospital would not normally be an affiliated person. However, a person hired to paint a hospital's record room who is required to move patient files while painting would be an affiliated person because access to those records is possible.[83]

A health care provider or other health information trustee may have a variety of relationships with service providers who have access to protected health information. When there is a contract, as there would be with a computer service provider, it is easy to identify the relationship with the affiliated person. With a regulated service like telephone service, there may be a contract or a tariff.[84]

---

[83] A painter who merely had to pass through the record room on the way to another location would not have to be treated as an affiliated person. Similarly, a fireman who may enter a hospital record room while putting out a fire does not become an affiliated person. Brief, incidental, or theoretical access to records does not make a person an affiliated person under the Act.

In the case of the painter passing through the record room, the presence of supervision that would prevent the possibility of access to patient records would be another factor suggesting that no access to actual records was part of the painter's function and therefore no affiliated person relationship was created. The affiliated person concept should be applied in a reasonable manner, with the focus being on whether access to identifiable records is a part of the activity involved.

[84] It is possible that a tariff might be wholly sufficient to define the role of an affiliated person under the bill. Consider, for instance, a common carrier telephone service provider that is re-

But things are not always as clear. As a result, the definition of "affiliated person" has been deliberately left open-ended and nonformal.

The affiliated person may be someone associated with a trustee but who does not have a formal legal relationship. For example, a medical student or hospital volunteer may be an affiliated person although neither may have a contract with the hospital. Employees of physicians or other providers located in a hospital but who are not themselves employees of the hospital may be affiliated persons if they have access to hospital patient records. In these instances, the affiliated persons may be subject to the same protected health information rules, training, and procedures as direct hospital employees.[85]

Affiliated persons will include a wide range of private organizations such as service bureaus, third party administrators, claims processors, auditors, and others who collect, automate, retain and use protected health information to provide services to trustees. The emergence of health information organizations is a response to needs of trustees. The Fair Health Information Practices Part is not intended to control the development of these organizations; it is only intended to control use of protected health information.

An affiliated person, like an employee of a trustee, does not have unlimited access to protected health information. Access is still regulated by the general principle that all uses and disclosures must be limited when practicable to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed.

The term "health care" is broadly defined in the bill to include any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to (I) the physical or mental condition or functional status of an individual or (II) affecting the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue. The term also includes any sale or dispensing of a drug, device, equipment, or other item to an individual, or for the use of an individual, pursuant to a prescription.

The term is intended to be broadly encompassing and to include the results of genetic tests on an individual or his or her future offspring. With the ability to conduct genetic tests that may indicate information about future offspring, a narrow interpretation could exclude the results of such genetic tests. This is not the intent of the legislation. Such genetic tests clearly fall within the scope of preventive, diagnostic, or therapeutic care, counseling, service, or procedure. Genetic counseling is also included within the definition of health care.

---

stricted by tariff, regulation, or statute from access to or use of the content of a telephone call. A trustee may find that the role of the telephone service provider with respect to any protected health information transmitted in such a call is fully described as a result. Any possible duty or authority of an affiliated person may be foreclosed by a lack of effective access to the underlying data. If not, a supplemental agreement may be required.

[85] Formal non-disclosure agreements between health care facilities and students, volunteers, contractors, and vendors are not unusual. For examples of these agreements, see Brandt, Maintenance, Disclosure, and Redisclosure of Health Information (American Health Information Management Association) (1993).

The definition of "health care" excludes any item or service that is not furnished for the purpose of maintaining or improving the health of an individual. This exclusion is intended to cover the collection of health information outside of a treatment relationship or the payment process. For example, information about an individual's physical condition that is collected by a physician during an examination conducted on behalf of a life insurance company as part of an application for life insurance does not fall within the definition because the physician is not providing treatment. The physician is, instead, collecting information with the consent of the individual for transmission to a third party. Likewise, information about an individual's physical condition collected by a researcher in the course of research when no treatment is provided would not fall within the definition.[86] There is no physician-patient relationship, no expectation of confidentiality under the Part, and, more importantly, no treatment. Similarly, information about medical condition shared with a hairdresser ("My hair is falling out because of radiation treatments for cancer") is not covered because there is no nexus to health treatment or payment.

When there is a treatment relationship, all information generated, collected, or retained pursuant to the treatment is part of the health care process and falls within the scope of the definition. The definition should not be read so that specific items of information can be determined not to be for treatment while other items fall within the definition.

The terms "disclosure" and "use" are employed to refer to the sharing of protected health information by a health information trustee. A use occurs when a health information trustee utilizes protected health information or provides access to an officer, employee, or affiliated person of the trustee. A disclosure occurs when access to protected health information is provided to any other person. In essence, the bill distinguishes between internal uses and external disclosures. When protected health information is provided to the individual who is the subject of the information, the access is neither a use nor a disclosure.

The bill sets out all of the disclosures that a health information trustee is authorized to make. Permissible uses are determined by the application of a standard set out in section 5131 of the bill. The distinction between internal uses and external disclosures will not always be obvious. Consider a hospital that is affiliated with a university. Access to protected health information by the executive director of the hospital in connection with management of the hospital would be an internal use. The determination is harder when considering the possibility of access by the president of the university, counsel to the university (as distinguished from counsel to the hospital), or university fund raisers. Whether any of these people can justify access to information under the standards of the Fair Health Information Practices Part is a separate question. The initial question is whether to consult the list of permissible external disclosures or to consult the rules for evaluating internal uses.

[86] Researchers may be bound by other confidentiality laws or by their own agreements with patients. Nothing here is intended to suggest that these obligations may be ignored. The point is that the Fair Health Information Practices Part does not apply unless the information is collected for treatment.

In the case of the university and university hospital, the issue of internal versus external depends on how the trustee qualifies as a trustee. The hospital is a health information trustee because it is a health care provider. The rest of the university does not provide health care and should not be considered as part of the same entity for purposes distinguishing between use and disclosure. It is possible, however, that other parts of the university could qualify as affiliated persons. For example, the counsel to the university might be an affiliated person if supporting a function of the hospital that requires access to identifiable health information. However, if the counsel is seeking protected health information to carry out an unrelated activity of the university, then the access would have to be evaluated as an external disclosure.

The same principles apply when health care providers practice through a corporate structure. The provider may have a parent corporation, subsidiaries, and other associated corporate entities. In this context, the provider is the health information trustee because it is the provider that undertakes the activity that gives rise to obligations under the legislation. The release of protected health information to parents, subsidiaries, and related corporate entities will almost always be an external disclosure rather than an internal use. Associated corporate entities could be affiliated persons if they assist the hospital in carrying out its functions. However, if in pursuit of general corporate objectives, the parent corporation asked each of its hospitals to compile a list of patients with particular ailments or who were using particular drugs, the release of protected health information to the parent would be an external disclosure and would almost certainly be improper.

The lines in this area will not always be black and white. Any doubts should always be resolved in favor of limiting access to protected health information. The interests of the individuals whose records are at issue should always be the paramount consideration.

SECTION 5121. INSPECTION OF PROTECTED HEALTH INFORMATION

It is a basic element of any code of fair information practices—as well as an essential element of fundamental fairness—that individuals have a right to see their own records. In a recent public opinion poll, 96% of the public said it was important that individuals have the legal right to obtain a copy of their own medical records.[87] According to Professor Alan Westin, people do not have that right today in 23 states.[88]

A statutory procedure for patient access to health records may actually be a cost saving measure. While not all states require that patients be provided a copy of their records, a determined patient will almost always be able to obtain a copy through litigation. By permitting access without litigation, the same result will be achieved without unnecessary expense. Access will no longer be limited to patients with the knowledge to seek or ability to pay a lawyer.

---

[87] See Louis Harris and Associates, Health Information Privacy Survey 1993.

[88] Testimony of Dr. Alan Westin, Professor of Public Law and Government, Columbia University, at H.R. 4077 Hearings (April 20, 1994). See also Public Citizen Health Research Group, Medical Records: Getting Yours (1992).

There are other potential savings as well. The 1973 report of the Commission on Medical Malpractice established by the Secretary of Health, Education, and Welfare included this finding:

The Commission finds that the unavailability of medical records without resort to litigation creates needless expense and increases the incidence of unnecessary malpractice litigation.[89]

The Commission recommended that medical record information be made more easily accessible to patients.

There is also some evidence that access may result in better treatment, improved patient education, and a more open doctor-patient relationship.[90] The evidence on this point in incomplete, and the Committee is not recommending patient access because of medical advantages. There are other reasons that more than adequately justify patient access.

Another consequence of patient access may be a reduction in medical expenses. In 1979, a witness testified that his family had moved eight times in nineteen years and that despite his best efforts, he was unable to accumulate all of their medical records and keep them current. As a result of the inability to retrieve earlier records, a family member had to redo expensive medical tests.[91] Improved information technology may lessen the need for patients to manage their own records, but it will be a long time before the benefits of computerization will be fully realized. There will be paper records and potential savings for the foreseeable future.

The cost of providing for patient access to health information is likely to be small. In 1980, the Committee reviewed the experience of Federal agencies in complying with a similar access requirement under the Privacy Act of 1974. That Act had been in effect for several years at the time of the review. The Committee heard from several different components of the Department of Health, Education, and Welfare that were directly involved in the provision of health services. No problems with patient access were reported, and the rate of patient requests was approximately one per one hundred patient encounters. The cost of complying with access and correction provisions very similar to those in the Fair Health Information Practices Part was found to be about $700 per facility in the late 1970s.[92] The Committee anticipates that the cost of complying with the patient access provisions will be minimal and that the benefits, while harder to measure, should exceed the costs.

Section 5121 of the Fair Health Information Practices Part requires health care providers, health benefit plans, health oversight agencies, public health agencies, and health information service organizations to permit an individual to inspect any protected health information about the individual that the trustee maintains and to bring another individual along during the inspection. An individual

---

[89] Department of Health, Education, and Welfare, Report of the Secretary's Commission on Medical Malpractice 75 (1973).

[90] See, e.g., Stein et al., "Patient Access to Medical Records on a Psychiatric Inpatient Unit", 136 American Journal of Psychiatry 327 (1979); Golodetz et al., "The Right to Know: Giving the Patient His Medical Record", 57 Archives of Physical Medicine and Rehabilitation 78 (1976); Shenkin and Warren, "Giving the Patient His Medical Record: A proposal to Improve the System", 289 New England Journal of Medicine 688 (1973). See also Novack et al., "Changes in Physicians' Attitudes Toward Telling the Cancer Patient", 241 Journal of the American Medical Association 897 (1979).

[91] 1979 "House Hearings" at 941–2 (testimony of Leon Troyer).

[92] See House Comm. on Government Operations, Federal Privacy of Medical Information Act, H.R. Rep. No. 96–832 Part I, 96th Cong., 2d Sess. (1980) (report to accompany H.R. 5935).

also has the right to have a copy of the information. The right of inspection and copying includes paper records, computer records, x-rays, and any other type of protected health information regardless of form or medium. The right of inspection also includes any accounting required under section 5124 and a copy of an authorization as required under section 5132.

The trustee has the right to offer to explain or interpret information provided to the individual. No trustee is required to provide an explanation, but it may be in the best interest of both the trustee and the subject of the records if an explanation is offered. Health records can be complex documents, filled with abbreviations and data that is unintelligible to the layman. Explanations will facilitate understanding, improve relations, and avoid needless anxiety and litigation.

The right of inspection applies to the major classes of trustee who use health information to make determinations about people. Both providers and benefit plans have direct contact with individuals and make decisions about treatment and payment. Health oversight agencies also must permit inspection and copying because their activities may also have a direct effect on individuals even though the agencies may not normally be in contact with the individuals. Nevertheless, a decision by an oversight agency to disallow a claim could have a devastating financial effect on a patient, and fundamental fairness requires that there be access to the underlying records. Public health authorities also may use health information about individuals to make decisions with serious consequences. For example, a public health authority can place an individual in quarantine. Access to records is therefore important.

There are seven categories of information that can be withheld from an individual. Reliance on these exemptions to access is optional. No trustee is required by anything in section 5121 to withhold the information that falls in one of these categories. There may, however, be other legal or professional obligations that warrant withholding.

First, a trustee may withhold mental health treatment notes if the trustee determines in the exercise of reasonable professional judgment that access to the notes would cause sufficient harm to the subject of the notes so as to outweigh the desirability of permitting access. This is permitted in order to protect the delicate relationship between therapists and patients and to recognize the existing practice whereby such notes are closely protected by the therapist from all non-treatment uses. Notes might include the therapists's speculations, impressions, hunches, and reminders, but would not include objective medical information such as test results, diagnoses, types of treatment provided, and similar information.

Another prerequisite for denying access to mental health treatment notes is that the trustee does not disclose the notes to any person not directly engaged in treating the individual, except with the authorization of the individual or under compulsion of law. Thus, if the notes are maintained in a general record that can be routinely seen by non-treatment personnel, the exemption to access will not be available.

82-256 0 - 94 - 4

It is the policy of the legislation that permitting access to records is generally desirable. As a result, the burden of justifying the withholding of mental health treatment notes falls on the provider/trustee. A specific determination is required in each case, and the provider/trustee must be able to articulate the harm that would result from access.

The bill places the responsibility for making the determination to withhold on the trustee. In some cases, the trustee will also be the health care provider. In other cases, the provider will be an employee or person otherwise affiliated with the trustee. Obviously, decisions that require professional judgment are best made by the professionals who are involved in the treatment of the record subject. The Committee expects that these professionals will normally be consulted. Where the original health care provider is no longer available, trustees will have to make the necessary judgments using other available professionals.

The second category of information that can be withheld from an individual is information that relates to other individuals. In order to withhold this type of data, the trustee must determine in the exercise of reasonable professional judgment that access would cause sufficient harm to one or both of the individuals so as to outweigh the desirability of permitting access.

The Working Group on Ethical, Legal, and Social Implications of the Human Genome Project has suggested that genetic information raises special problems because information about an individual also relates to the individual's blood relatives who may carry the same genes. The fact that information about a requester also pertains to the requester's relatives does not create a basis for withholding information about the requester from the requester. Similarly, while information that is in the file of a relative may have some bearing on a requester, the requester does not have a right to see any information that does not pertain directly and specifically to the requester. In general, where information about one individual is maintained in a file about another individual, the first individual's inspection and correction rights are limited to his or her own file. If information in another file is not used to make decisions that affect an individual, then access and correction are not required.

The third category of information that can be withheld from an individual is information that could reasonably be expected to endanger the life or physical safety of an individual. This exemption is not likely to be used often, but it could be very important in those few instances where it is available.

The fourth category of information that can be withheld from an individual is information that identifies or could reasonably lead to the identification of an individual who provided information under a promise of confidentiality to a health care provider concerning the individual who is the subject of the information.[93] This exemption cannot be used to withhold the identify of a health care pro-

[93]The Privacy Act of 1974, 5 U.S.C. §552a (1988), makes a distinction between express and implied promises of confidentiality. After the effective date of the Privacy Act, a promise of confidentiality is only effective if it is an express promise. For information collected prior to that effective date, an implied promise of confidentiality is sufficient. See 5 U.S.C. §552a(k)(2) (1988). This same distinction between express and implied promises is appropriate for the Fair Health Information Practices Part.

vider who is involved in the treatment of the individual. But there may be circumstances in which family members or others provide information to health care professionals on a confidential basis. For example, a woman who tells a physician about her husband's condition or activities might not want her husband to know that she was the source.[94]

The fifth category of information that can be withheld from an individual is information that is used by a trustee solely for administrative purposes and not in the provision of health care to the individual who is the subject of the information. If the information is disclosed to any other person, then this exemption is not available. Use of the information by the trustee and its employees does not make the exemption unavailable. Examples of qualifying information are operating room schedules and patient lists that may be used for administrative purposes. Billing information cannot qualify under this exemption.

The sixth category of information that can be withheld from an individual is information that duplicates information that is available for inspection. If copies of x-rays, pathology reports, lab results, or similar items are maintained in several different places by a trustee, only one copy must be made available to the subject provided that all copies are identical. If the copies differ in any way or some include handwritten notes, then all must be provided.[95]

The seventh category of information that can be withheld from an individual is information that is compiled principally in anticipation of a civil, criminal, or action or proceeding or that is compiled principally for use in such an action or proceeding. This incorporates the attorney-client evidentiary privilege.

If a trustee denies a request for inspection or for copying in whole or in part, the trustee is required to give the individual a written statement of the reason for the denial. This follows the policy of the Freedom of Information Act. A trustee must disclose when information has been withheld and why it has been withheld. The statutory deadline for complying with requests is 30 days beginning on the date the trustee receives the request.

The exemptions in the bill apply only to the access and inspection process under section 5121. The exemptions do not apply in other circumstances. For example, if a patient brings a malpractice action against a physician and seeks a copy of all of the physician's records pertaining to that patient under the discovery rules of the court, the exemptions in the Fair Health Information Practices Part are not applicable or relevant. The scope of the patient's right to the record will be determined solely under the applicable discovery rules. The Part's exemptions do not apply and are not intended to interfere with or to limit any other access rights or procedures that may be available to the subject of the record under other laws or policies.

A trustee may establish reasonable procedures governing requests for access and inspection. Section 5121 specifically allows a

---

[94] See, e.g., Burnum, "Secrets About Patients", 324 New England Journal of Medicine 1130 (April 18, 1991) ("Doctors are often given information about a patient by family members or other and asked to keep it secret from the patient.").

[95] When corrections are made, the correction must be included in all copies of the incorrect information. The exception for access to duplicate records should not be read to extend to corrections.

trustee to require a written request for access. Of course, a trustee may require that an individual seeking access provide sufficient identification. Requiring fingerprints or other expensive, cumbersome identification methods that are intended to serve as a procedural barrier to access is not appropriate or permitted. The identification requirement must be reasonable.

If a trustee relies on any of the exemptions to deny access, the trustee must permit access to any reasonably segregable portion of a record after deletion of any exempt portion. This is a standard policy borrowed directly from the Freedom of Information Act.[96] It prevents a trustee from withholding an entire record or even an entire page just because there is one line of exempt information.

A trustee may charge a reasonable cost-based fee for permitting inspection or for providing a copy. A fee is not required,[97] and a trustee may permit inspection or provide copies at no charge or at a reduced charge. The fee permitted under this section applies only to first person access. Copying or other charges imposed on other users of health information are not regulated. A trustee may have a different fee schedule for records that are provided to insurers, providers, lawyers, or others. Only those requests made under section 5151 are subject to the reasonable cost-based fee standard.

The fee must be reasonable. The overall intent is to provide for patient access at the lowest possible fair price. Providing patient access is not intended to create a profit center for health information trustees nor is it intended for trustees to lose money responding to patient requests.

There is a cost associated with each patient request for access or for copying, but the section does not require a trustee to calculate the actual cost for each request. The fee must be cost-based. A cost-based fee must be related to the costs of responding to requests, but a trustee is not required to track each cost element for each request. A trustee may choose to base its fees on the average cost of retrieving a record, copying a page, or duplicating an x-ray.[98]

There are several elements for which costs may be recovered. For example, there are labor costs associated with processing requests, retrieving records, and copying records. There are costs for materials and equipment that may include computer time, photocopying charges, paper, and similar items. There may be postage costs, administrative expenses, and other expenses that are directly related to responding to requests. A trustee may hire a contractor to perform some or all of these functions and may pass on the contractor's charges to the patient, provided that the charges are reasonable and consistent with the standard in the section.

A trustee may not charge an arbitrary fee unrelated to the trustee's cost. For example, a hospital may not impose a fee for a copy

---

[96] 5 U.S.C § 552(b) (1988).

[97] There are some states that provide for reduced fees for patient inspection or copying. These state policies are not altered by the preemptive nature of this section because the charging of fees is discretionary with the trustee. Where discretion may be exercised in this area, it is not inconsistent with the preemption language if the discretion is exercised by the state or by the trustee. The framework of the inspection section remains intact.

[98] A determination of average cost can be made in a number of ways. A trustee may evaluate its own costs, may determine average costs in association with other trustees in the same city that perform similar activities, or may use general office cost studies for similar function in its region. The Act does not require an elaborate cost-accounting justification for each action. The process used to calculate average cost need only be reasonable and not exact.

of a bill that is a percentage of the bill. That would violate the requirement that the fee be cost-based. If records are fully computerized, the costs of providing a digital copy may be small, and fees should reflect the lower cost. For example, when it is necessary to physically retrieve a paper record from a central repository, there may be a charge for the retrieval. But if the retrieval of a computerized record can be accomplished through a few keystrokes, it would be unreasonable to impose the same retrieval fee as for a paper record because the costs are significantly different.

SECTION 5122. AMENDMENT OF PROTECTED HEALTH INFORMATION

The right to seek correction of records is another basic element of a code of fair information practices. Section 5122 imposes a requirement to accept and consider requests for amendment on the same health information trustees who are required to provide for patient inspection. The requirement applies to health care providers, health benefit plans, health oversight agencies that maintains protected health information and to health information trustees who receive protected health information pursuant to section 5141 (health information service organizations).

A trustee has forty-five days to make a decision on a request for amendment. If the trustee makes the requested change, the trustee must make reasonable efforts to inform any person (other than an employee of the trustee) identified by the subject of the record who is a known recipient of the incorrect information about the change. The purpose here is to make sure that improper information passed on to others is accurate and up-to-date. The accounting for disclosures required under section 5124 will provide a list of potential recipients of the data. It may not be necessary to provide the correction to all recipients.[99] The trustee is also required to make reasonable efforts to inform known sources of incorrect information.

The requirement that *"reasonable efforts"* be made to share corrections means that trustees must try to contact the persons who are to receive the corrections. In most circumstances, use of the mail or the telephone will be sufficient. How much effort is required will depend on a number of factors, including the age of the incorrect information; the expense involved; and the importance of the correction. If a record has been changed because it indicates an incorrect blood type, it is appropriate that greater efforts be made to ensure that the correction is received by all who have the wrong information. Incorrect information of this type could result in serious harm.

On the other hand, lesser efforts may be appropriate when a record is corrected to show that a patient is actually 42 years old and not 43 years old. Also, a correction need not be provided where it would serve no purpose. For example, if a physician was a source

[99] It is possible that sending corrections to some recipients will not be necessary or appropriate. For example, suppose that a data tape containing hundreds of patient records is accidentally mailed to the wrong address. Technically, the records were disclosed to that accidental recipient. Sending corrections to that same recipient would be pointless and would actually exacerbate any improper disclosure. Presumably, the record subject would choose not to have a correction sent in such a circumstance. There may be other cases where the record subject would not choose to send the correction. A trustee may, however, transmit a correction to a previous recipient if the trustee decides that the disclosure is appropriate and otherwise consistent with the Act.

of information but is no longer in practice, providing a correction to that physician would be pointless. Where reasonable attempts fail without satisfying the patient, a trustee may provide the patient with a certified copy of the changed record and the patient may pursue the dissemination of the corrected record as he or she sees fit.

Overall, section 5122 allows health information trustees considerable procedural flexibility. When a trustee denies a request for change or amendment, the trustee must inform the individual of the reasons for the refusal and of any procedures for further review. A trustee is not required to conduct hearings or to have an internal appeal procedures, but the existence of an appeal procedure must be disclosed to requesters. The burden of proving that information maintained by a health information trustee needs to be amended or corrected falls on the patient. If the trustee decides that a patient has failed to meet this burden, then the request may be denied.

Section 5171(f) provides elsewhere that a requester must exhaust any administrative appeal procedure before pursuing judicial remedies. It is possible that trustees may jointly establish appeal mechanisms to consider appeals. For example, hospitals in a region may utilize an appeal process established and operated jointly by the hospitals or they may utilize an independent review service. The alternative dispute resolution mechanisms described in section 5173 may be applied to correction appeals.

If an individual's request for correction is denied, the individual has the right to file with the trustee a concise statement setting forth the requested correction and the individual's reasons for disagreeing with the refusal. Any statement of disagreement must be included in any subsequent disclosure of the disputed portion of the information about the individual. The trustee may include a concise statement of its reasons for not making the requested change. This is similar to an existing requirement under the Privacy Act of 1974.

An individual may request correction or amendment of protected health information about the individual when the information is not timely, accurate, relevant, or complete for the purposes for which the information may be used or disclosed. The standard of timely, accurate, relevant, and complete is common in codes of fair information practices. The requirement for correct records must be assessed in light of the purposes for which the information is being used or disclosed. For example, a hospital record can be a dynamic document, with information being added constantly during and after an inpatient stay. Such a record cannot be judged to violate the statute's timeliness standard simply because information has not yet been added. Only when a delay in posting information is unreasonably long or a patient is prejudiced as a result of an abnormal delay, then the record may be found to be in violation of the standard. In many cases, a professional judgment about timeliness, accuracy, relevance, and completeness will be appropriate.

Similarly, a record may include information that a physician was told by a patient (e.g., "My husband hit me when he was drunk"). It is not the obligation of the physician to determine the truth of the statement. If the physician deems the statement to be relevant

and includes it in the record, the physician has no obligation under the Fair Health Information Practices Part to investigate the truth of the statement. The record is correct if it is an accurate and relevant reflection of what the patient said. A patient, of course, may seek to add a statement disagreeing with the accuracy of the record.

There is considerable case law under the Privacy Act of 1974 where individuals attempted to use the Act's correction mechanism as a basis for collateral attacks on agency determinations. The courts have generally rejected these attempts. This line of reasoning is fully applicable here as well.

It is standard practice for a medical record keeper not to expunge any information in a treatment record. The universal procedure is to mark incorrect information and to add the correct information. Section 5122(e) makes it clear that there is no requirement that any information be erased or deleted. The trustee is expressly authorized to mark incorrect information and to place supplementary correct information in the record and to add appropriate cross references to the correct information. This strict policy for medical records may or may not be needed for other types of records subject to the Part, but each trustee has the option to use the same correction procedure.

SECTION 5123. NOTICE OF INFORMATION PRACTICES

The Fair Health Information Practices Part relies on individual action as one enforcement mechanism. As a result, it is critical that individuals be informed about their rights and how to exercise them. This is also a standard feature of any code of fair information practices. Section 5123 accomplishes this by requiring some health information trustees to prepare and make available to any person a notice of information practices.

The requirement to prepare a notice of information practices falls on health care providers, health benefits plans, health oversight agencies, and health information service organizations. These are the trustees who will be making basic substantive decisions about an individual's health care and payment. Not all of these trustees will have regular and direct contact with individuals, but their activities are of sufficient importance that the notice must be prepared and made available upon request. The same duty has not been imposed on other health information trustees because there is not a sufficient nexus between the trustee and the subject of the information to warrant imposing the requirement of preparing a notice.

The notice must contain three elements. First, it must describe the rights that individuals have under the Part, including the right to inspect and copy information and the right to seek amendments. The notice also must describe the procedures for authorizing disclosures of information and for revoking authorizations.

Second, the notice must describe the procedures established by the trustee for the exercise of the rights provided by the Part. For example, a trustee who requires individuals seeking access to information to make a written request, to provide identification, or to pay an allowable fee in advance must describe the rules and procedures in the notice of information practices. If a trustee has estab-

lished an internal appeal procedure for denials of access or amendment, the procedure should be described in the notice. The notice should also include the name, address, and telephone number of the office that an individual should contact to exercise the right of access and amendment.

Third, the notice should describe the types of uses and disclosures that are permitted. This description of uses and disclosures does not have to be excessive in detail nor does each potential use and disclosure have to be spelled out in full. The purpose of the description is to make individuals generally aware of how the information they supply may be seen by others and to permit them to exercise the right to object to disclosures.

In order to assist in the preparation of the required notice of information practices, the Secretary is required to develop and disseminate model notices for uses by trustees. Several different types of notices will be necessary to meet the needs of the different trustees. A notice for a provider will be different from a notice for a payer or an oversight agency. Model notices will reduce the prospect of litigation over the sufficiency of the notice for any given trustee. While each trustee may have to adapt the model notice to meet its own situation, use of the core notice issued by the Secretary will provide a safe harbor.

The notice of information practices should be distributed to any individual upon request. There is no requirement that a copy of the notice be affirmatively handed to each patient, but a trustee who routinely sees patients must inform the patients of the availability of the notice. The posting of a sign stating the availability of the notice is one way to accomplish this. Patients can be notified in others ways as well, including through notices on bills or other written documents.

A trustee who does not routinely interact with patients, such as a health oversight agency, need only make efforts to inform individuals about the availability of the notice at the time when there is contact. There is no requirement that signs be posted at locations where patients do not routinely appear. Notice can be provided in other reasonable ways. One such way is to include a written statement on a form or other document that will be seen by patients.

SECTION 5124. ACCOUNTING FOR DISCLOSURES

Section 5124 requires that all health information trustees maintain an accounting for each external disclosure of protected health information. There are four required elements for accounting. First is the date and purpose of the disclosure. The second is the name of the person to whom the disclosure was made. This does not require recording the name of the specific individual who received the information. It is sufficient to record the institution to which the information was provided. Thus, an accounting might identify the person as "Blue Cross of California" or "Dr. Jane Doe's Office" or "University of Oklahoma Hospital".

The third element of the accounting is the address of the person to whom the disclosure was made or the location to which disclosure was made. In the modern information age, a street address is not always the most meaningful or relevant location, and it may not be known when at the time the data is disclosed. Much infor-

mation is shared through electronic means. A computer address may be appropriate. The goal is to allow the recipient to be found at a later date. The accounting should include the most appropriate location information under the circumstances.

When disclosures are routinely made to the same institution, the address does not have to be repeated each time in each record. If, for example, disclosures are routinely made to Blue Cross, it is sufficient that the location of Blue Cross can be provided when needed later.

The last element of an accounting is a description of the information disclosed, where practicable. This requirement should be interpreted in light of the technical capabilities of the system used to maintain the record and the cost of such maintenance.

This is not intended to require a specific recording of each data element disclosed. When it is practical and cost-effective to maintain more detailed data about the disclosure, then it is appropriate to do so. This may only be the case in an advanced computerized health information system that has such a capability built in. For existing computer systems with limited capability for accounting, the practicability standard does not mean that expensive reprogramming is required. These systems may be accepted as they are if a basic set of accounting data is maintained in some fashion. The accounting information may even be maintained in a separate system or on paper.

The Secretary may decide to establish more specific accounting requirements through regulation. The Secretary could, for example, prescribe rules for computer systems that will be placed in service at a future date. By establishing such requirements well in advance, the needed capabilities can be designed and implemented at low cost and without the need for retrofitting.

For paper records, practicalities and expense will limit the description of the information disclosed. If an entire record is disclosed, then the accounting may so note. The possibility that the record will change in the future is not important, even though it may be impossible to determine exactly what data elements were disclosed. Since it is not practicable to track individual data elements for paper records, the accounting may be more broadly descriptive because the cost of recording details is prohibitive.

The accounting for disclosures is itself protected health information, and the Section 5121(a) expressly provides that the individual is entitled to see the accounting for disclosures made from the record about the individual. This is one way that an individual whose rights have been violated by an improper disclosure can identify the responsible party.

The accounting provision does not require any specific type of form or log. As long as disclosures can be identified or accurately reconstructed, a trustee may maintain the accounting in any way that it chooses. Accounting information can be included in a patient file, in a separate log, or in any other way. As long as it is possible to provide the basic elements to a patient who requests them, then a trustee can choose a method most suitable to its record keeping practices.

No accounting is required for disclosures made under the next of kin and directory information section. The recording of these disclo-

sures would be unduly burdensome or otherwise unnecessary. Similarly, the Secretary is directed to issue regulations exempting from the accounting requirements disclosures for purposes of peer review, licensing, certification, accreditation, and similar activities. These types of activities generally do not involve the review of specific patient records in connection with determinations about the patient. An accrediting agency may review records only to determine if general record keeping standards are being met. Requiring an accounting would normally be unnecessary. The Secretary's regulations can provide more detailed rules.

SECTION 5125. SECURITY

Section 5125 requires each health information trustee to maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of protected health information against any reasonably anticipated threats or hazards. Key words in the security section are "reasonable", "appropriate", and "reasonably anticipated". Trustees are obligated to maintain security, but they are not expected to provide absolute protection against all possible security breaches. Nevertheless, casual security measures will not meet the statutory standard. Each trustee must be sure that it has an adequate security plan and that its employees have been trained to recognize the special obligations that attach to protected health information.

The statutory requirements have intentionally been stated very broadly. Section 5125 requires the Secretary to develop and disseminate security guidelines. It is not appropriate to specify appropriate security methods in legislation because technology is too varied and too dynamic. Additionally, different types of technology call for different types and degrees of security. For example, the same security measures may not be appropriate for information maintained on paper as for information maintained on computers. Paper records, computerized records, and networked records all face different types of threats.

The Secretary's guidelines can take all these factors into account. They can consider the technical capabilities of record systems, the costs of security measures, the need for training of personnel, and the value of audit trails in computerized record systems. Specific security measures, such as audit trails, are especially valuable for computer systems that have the capability of recording the necessary data.[100] It will be appropriate for the Secretary to direct that new computer systems should include the ability to maintain audit trails at some point in the future.

Another key security element is the need for sufficient resources so that security goals can be accomplished. For example, it is nice to have a computer system that maintains audit trails monitoring internal access to protected health information. But if the audit trails are simply recorded without any review of suspicious activity,

[100] An audit trail would record the date, identity, and information access for an internal use. Access by a hospital employee to a hospital patient computer system would be recorded through an audit trail. An audit trail is different than an accounting for disclosure. An accounting is appropriate when protected health information is disclosed to a person other than the trustee, an officer or employee of the trustee, or an affiliated person of the trustee.

then there is little meaningful security.[101] The adequacy of a trustee's security may be measured not only by the technical measures in place to prevent or monitor misuse but also by the effective use made of those security measures. A trustee who records misuse of information but who rarely or never investigates suspicious activity will not meet the statutory test of reasonable and appropriate measures. The Secretary can and should address the resource issue in more detail.

Security measures must protect against reasonably anticipated threats. The Committee cautions, however, against treating security as simply the need to prevent hackers or outsiders from obtaining access to protected health information. That is only one element. There is evidence to support the belief that an equal or greater threat comes from misuse of information by those who have access to the information during the course of their routine activities. Insider abuse is a characteristic of virtually every computerized system containing personal information, and it may, in fact, constitute the greatest security threat.[102] Adequate security for protected health information must offer reasonable protection against insider abuse.

SECTION 5131. GENERAL LIMITATIONS ON USE AND DISCLOSURE

Section 5131 sets out general rules on the use and disclosure of protected health information by all health information trustees. An internal use of protected health information by a trustee is permissible if the use is for a purpose that is compatible with and directly related to the purpose for which the information was collected or received by the trustee. The standard is not intended to interfere with essential uses of information in support of the activities for which a trustee obtained protected health information. It is intended to impose a strict prohibition against extraneous or unnecessary uses by a trustee and the trustee's employees and affiliated persons.

The language for assessing uses is based in part on the experience of the federal government with the Privacy Act of 1974.[103] The Privacy Act contains fair information practices that regulate the collection, maintenance, use, and disclosure of personal records by federal agencies. Internal uses under the Privacy Act are usually governed by subsection (b)(1), which permits the disclosure of personal information to officers and employees of the agency maintaining the record who have a need for the record in the performance of their duties.[104] This standard has long been identified as imposing virtually no barrier to internal use of personal records.[105] The Committee disagrees with the way that this provision has been im-

---

[101] See, e.g., General Accounting Office, "National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information" (GAO/T–GGD–93–41). GAO found that some of the audit trails maintained as part of the NCIC system were reviewed infrequently and that abuse of information recorded in the audit trails was never identified as a result. See also OTA Medical Privacy Report at 54.

[102] Some technical measures that provide a degree of security—such as encryption—may be ineffective against insiders who have access to information before it is encrypted or after it is decrypted. Encryption may provide a higher level of security against external threats.

[103] 5 U.S.C. 552a (1986).

[104] 5 U.S.C. § 552a(b)(1) (1986).

[105] See, e.g., Privacy Protection Study Commission, "The Privacy Act of 1974: An Assessment" 69 (1977) (Appendix 4 to the Report of the Privacy Protection Study Commission).

plemented. Based on the experience under the Privacy Act, such a loose standard for internal uses of protected health information has been expressly rejected.

The Committee has also reviewed the Privacy Act's routine use provision that allows federal agencies administrative flexibility to define permissible disclosures. A routine use is the disclosure of a record for a purpose that is compatible with the purpose for which the record was collected.[106] This standard has also been interpreted much too loosely by the agencies. Most agencies view the routine use provision as permitting virtually any disclosure just as long as the proper notice has been published in the Federal Register. This view of the law is incorrect. The principal effect has been to treat the routine use provision as a procedural rather than a substantive barrier to disclosure. This was not the original intent of the Privacy Act, and there are many existing routine uses that are inconsistent with both the letter and the intent of the Privacy Act.

The Committee recognizes that it would be an impossible task to set forth in the legislation all appropriate internal uses for protected health information by all trustees. A general statutory standard is required. The "need to know" standard used in the Privacy Act was rejected as ineffectual. The Committee also rejected the simple compatibility test of the Privacy Act's routine use definition because it has proved in practice to be unacceptably unrestrictive.

Instead, the bill permits the use of protected health information only for a purpose that is compatible with and directly related to the purpose for which the information was collected or was received by the trustee. Each person or institution that becomes a health information trustee must apply this test to its activities. The key concept is that of "purpose". A trustee's purpose must be assessed on the basis of the reasons the protected health information was collected or received. Thus, a person who becomes a health information trustee by virtue of a disclosure under emergency circumstances would have a very narrowly constrained purpose. Only those uses that are compatible with and directly related to alleviating emergency circumstances would be permitted. Other uses are unrelated to the purpose of the trustee and would be prohibited, but internal uses that are essential to the management of the trustee are acceptable.

In contrast, a health care provider would have a much more expansively defined purpose. For example, in a hospital, the use of protected health information to support the provision of health care would obviously be permitted. Other uses that are necessary for the functioning of the hospital, for routine management activities, for quality assurance activities, or for carrying out mandates under law fall within the purpose for which the information was collected. Teaching, training, and research activities also can fall within a hospital's purpose.

In order to clarify the full range of permissible uses, the bill specifically provides that a trustee may use information for a purpose for which the trustee is authorized to make a disclosure. For example, a hospital can disclose information to an external health re-

---

[106] 5 U.S.C. § 552a(a)(7) (1986).

searcher who has met the standards of the health research section. The hospital may permit a researcher who is an employee to have the same access under the same conditions. Similarly, internal oversight uses that are the same as authorized external oversight disclosures are permitted under the same conditions.

One especially troublesome area involves the use of patient records for direct marketing. External disclosures for marketing are not authorized anywhere in the Fair Health Information Practices Part. Use by a hospital, for example, of its own patient list for its own direct marketing activities would have to meet the statutory test of compatible with and directly related to the hospital's purpose. Some uses will fall within the test. For example, contacting patients by mail to inform them that a provider has moved its location meets the test.[107]

Most other uses of patient information for marketing are likely to be inconsistent with the standard. The sale of patient lists of any type would be a disclosure and would be expressly prohibited. A mailing conducted by a trustee for a third party also would fail to meet the use test ("This hospital urges its patients to buy safe automobiles such as those manufactured by the XYZ Company") though there was technically no disclosure to the third party. This would simply represent a circumvention of the disclosure restriction.

Use of patient specific information for marketing activities was troubling for health industry witnesses as well. At a hearing on H.R. 4077, Frederic Entin, Senior Vice President and of the American Hospital Association discussed the marketing issue in more depth:

> We draw the line at selling of lists. That is something that should not occur. We have various advisories and documents that have been developed over the years that we disseminate to our members with regard to the overall question of confidentiality of records and use of records for a variety of purposes.
>
> I have reviewed those. I can't say that we have a direct position that opposes marketing in general. One could justify use of patient information in a hospital to the extent that the hospital is using that list of patients to inform them of services that are beneficial to members of the community.
>
> To go beyond that and to target patients for particular services because of their disease condition is something which doesn't need to be asked. It is a very difficult problem and you have to balance, I would suggest, the need to

[107] How the mail is sent may make a difference. The mailing of a postcard can involve the disclosure of patient information. For example, a clinic that exclusively treats patients for sexually transmitted diseases would certainly be ill advised to sent a postcard to all former patients announcing a new location. The fact that a particular individual was a patient of the clinic is protected health information, and the postcard might be read by a postal worker or any another members of the individual's household. The same notice sent in an unmarked envelope would not normally constitute a disclosure.

There is nothing in the Act that prevents the use of a postcard to contact a patient to notify the patient about an appointment if the patient has been notified of the practice and has not objected. A physician may ask if a patient objects to being notified by postcard and follow the patient's preference.

provide useful information to the community against the right to privacy.[108]

Dr. Donald Lewers, a Member of the Board of Trustees of the American Medical Association and another witness at the hearing, agreed with Mr. Entin:

> I think we agree. We still have to fall back to where we were as far as unique identification and associating that individual with release of that information. Sending an individual a letter is one thing but if you are using that information in identifying that patient, that is wrong.
>
> There are a lot of times where you need to get disease-specific information for tracing issues, certain diseases where you may have to go into that. But to market is a little different area that we have to be careful about, and I would agree with the previous speaker on that.[109]

Kathleen Frawley from the American Health Information Management Association offered an equally strong objection to the use of information for marketing: "I think that any use of an individual's information for direct marketing purposes should be authorized by that individual. I think that we have to be very careful about those kinds of practices."[110]

All of these witnesses agreed that marketing uses of specific patient information is improper. Selecting patients for mailings or similar marketing activities based on diagnoses, types of treatment, prescriptions, or similar information is inappropriate. Merging patient lists with other consumer mailing lists or other consumer profiles is similarly inappropriate.

The intent of the legislation is to draw a very tight line around the use of any protected health information by health information trustees for marketing. As Dr. Lewers pointed out, patient information may be needed for tracing certain diseases.[111] That would obviously be a treatment activity and does not constitute marketing. Other contacts with patients also may constitute treatment and may not be subject to restriction in this way. In general, however, any doubts about the use of protected health information for marketing activities should be resolved by denying use of the information. Any use of patient-specific information for marketing is simply inappropriate. The establishment or sale of mailing list or consumer profiles containing diagnoses, health information, drug usage, or similar information is offensive and an invasion of privacy.

Another general restriction on use and disclosure is the requirement that a use or disclosure of protected health information by a health information trustee be limited, when practicable, to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed. This applies to all

---

[108] H.R. 4077 Hearings (May 4, 1994).
[109] Id.
[110] Id.
[111] Id.

uses and to all permitted disclosures, including disclosures made pursuant to discovery, subpoena, and warrant.[112]

The Secretary is required to issue guidelines to implement this restriction, and the guidelines must take into account the technical capabilities of the records systems used to maintain protected health information and the costs of limiting uses and disclosures. These are the principal factors to be considered in making practicability determinations. For example, it is likely to be easier to be much more specific when providing access to computerized records than when providing access to paper records. A well-programmed computer can automatically permit each user to see only that information that is needed to accomplish the user's purpose. This type of restricted access can be prohibitively expensive for routine activities when records are maintained on paper, and the Secretary's guidance should take this into account. Other factors that are relevant to practicability determinations are the sensitivity of the information [113] and the nature of the use or disclosure. [114]

SECTION 5132. AUTHORIZATIONS FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION

Section 5132 provides that any person who seeks from an individual an authorization for the disclosure of protected information must provide the individual with a statement of the uses for which the person intends the information and of the disclosures that the person intends to make of the information. A statement that the person may disclose the information to any person and for any purpose is not specific enough to meet the requirement of the section. The purpose is to inform the individual how the information will be used or disclosed in fact and to restrict the recipient from using or disclosing the information without limit.

The statement of uses of disclosures must be provided to the individual before the authorization is executed, and the statement must be on a form that is separate from the authorization. The reason for the separate form is to allow an individual to authorize disclosure without disclosing the reason to the trustee. This may protect a privacy or other interest of the individual.

The statement of uses and disclosures is binding on the person who sought the authorization, and the person is subject to suit under the civil actions section with respect to any failure to comply.

---

[112] See, e.g., *Hawaii Psychiatric Society* v. *Ariyoshi*, 481 F. Supp. 1028 (D. Hawaii 1979) ["There has been no showing, and the court does not believe that there could be a showing, that the issuance of warrants to search and seize the therapeutic notes, patient history forms, diagnoses, and other confidential medical records of a psychiatrist, absent even a suspicion that an individual provider has defrauded the State or failed to maintain records, is necessary to serve any of the State interests put forward." Id. at 1041.]

[113] See, e.g., *Hawaii Psychiatric Society* v. *Ariyoshi*, 481 F. Supp. 1028 (D. Hawaii 1979) ["The private information disclosed to the State in Whalen consisted of the patient's name, age, address, and use of a certain drug. Here, the degree and character of the disclosure is far more intrusive. The psychiatrist's records may include the patient's most intimate thoughts and emotions, as well as descriptions of conduct that may be embarrassing or illegal." Id. at 1041].

[114] In *Commonwealth* v. *Korbin*, 479 N.E.2d 674 (1985), the Supreme Judicial Court of Massachusetts found that a grand jury subpoena issued in connection with an investigation of Medicaid fraud for the complete records of a psychiatrist was overly broad and that the details of a patient's problems are not necessary to an evaluation of whether a psychiatrist is rendering services in the amount claimed. The court imposed limits on the type of information that could be disclosed. The result in this case—and in similar cases decided elsewhere—is fully consistent with the policy of the Fair Health Information Practices Part that disclosures be limited to the minimum amount of information necessary to accomplish the purpose. In fact, the case is an excellent example of the minimum disclosure rule in operation.

In order to assist in the execution of authorizations for standard purposes, the Secretary is required to develop and disseminate model statements of intended uses and disclosures. The Committee anticipates that the Secretary will develop model statements for life insurance, malpractice litigation, and other routine activities. A person who uses the Secretary's model statement may so inform individuals (as provided in the Secretary's rules) and thereby offer a degree of reassurance that information will be properly used.

A health information trustee may disclose protected health information pursuant to an authorization executed by the individual who is the subject of the record. Any individual may authorize a health information trustee to disclose protected health information to any person. There are no restrictions in the legislation on the class of recipients or on how those recipients may use the information (other than the required statement of uses and disclosures). With the approval of the subject of the record, information may be disclosed to anyone and used in any fashion. However, a person who is entitled, qualified, or potentially qualified to receive protected health information pursuant to the statutorily authorized disclosures may not use the authorization process to avoid, evade, or diminish any of the requirements or restrictions in the Part. For example, a health researcher may not use the authorization process to evade the requirement that a health research project be approved by an institutional review board.

There is nothing in the Fair Health Information Practices Part that requires a health information trustee to comply with an authorization from an individual. A trustee may, in its discretion, refuse to make a requested disclosure that is not otherwise required by law. Of course, a trustee may not refuse to comply with an individual's request for a copy of his or her own record under section 5121. A trustee may impose additional reasonable requirements on the authorization process. For example, a trustee may impose its own reasonable identification requirements for authorizations, including notarization if appropriate. There may be other procedural rules regulating the time, place, and manner of presentation of authorizations. In addition, a trustee is not restricted in its ability to charge a fee for disclosure or reproduction of records pursuant to an authorization.

A health information trustee may disclose protected health information pursuant to an authorization that has been executed by the individual who is subject of the information and that meets eight requirements. First, the authorization must be signed and dated on the date of the signature. Normally, the authorization will be in writing, but electronic authorizations may be used in the future, and there is no requirement for a written document.

Second, an authorization may not be included on a form used to authorize or facilitate the provision of or payment for health care. Disclosures for payment are provided for elsewhere in the Part, and there may be no routine need for authorizations for this purpose. The requirement for a separate form is to prevent the unwitting execution of authorizations for other purposes while seeking payment of claims. For example, this requirement would prevent an unscrupulous person from obtaining an authorization for the

use of patient information for direct marketing on a claims form or other routine document.

Third, an authorization must be specifically named or generically described in the authorization form. An authorization that identifies any health care provider is acceptable.

Fourth, the person to whom the information is to be disclosed must be specifically named or generically described in the authorization form as a person to whom the information may be disclosed. An authorization form that identified the "bearer" is not sufficient to meet the requirements of this section. It is acceptable to identify a company (e.g., "Blue Cross") or law firm—rather than a named individual at the company or firm—as the recipient.

Fifth, the authorization must include an acknowledgement that the individual has received a statement of uses and disclosures. This will serve as a notice to the individual that he or she should have received such a statement.

Sixth, the information to be disclosed must be described in the authorization. Ideally, an authorization will list a particular item, such as a pathology report or discharge summary. A more general description might be "all records related to a specific hospitalization." An authorization may request the release of any or all information about the individual, although it is preferable that a request be more narrowly focused. In the end, this will be up to the individual. A trustee who receives a request for all information may, of course, choose to release a subset of that information. For example, a provider of psychiatric services may require a more specific authorization for the disclosure of mental health treatment notes.

Seventh, the authorization must be presented to the trustee in a timely fashion. For an authorization that permits disclosure to a health care provider, health benefit plan, health oversight agency, public health authority, health researcher, or person who provides counseling or social services, an authorization must be presented to the trustee within one year of the date it was signed by the individual. An authorization directed at any other person is only good if presented within thirty days of signature.

Eighth, a disclosure pursuant to an authorization must be made in a timely fashion. This means that the disclosure must occur before any date or event (if any) specified in the authorization upon which an authorization expires. A trustee who received an authorization in a timely fashion has six months to comply with the disclosure request. Thus, if an authorization that expires on March 2 is received by a trustee on March 1, the trustee may comply with the request even though the information will be disclosed after March 2. In this case, the trustee could make the disclosure anytime before September 1. This flexibility is a recognition that it will take a trustee time to identify, retrieve, and copy records.

An authorization may be revoked or amended at any time by the individual who executed it. There are two exceptions. Where a disclosure was authorized to permit validation of expenditures based on health condition by a government authority, the individual may not revoke authorization. It would be inequitable for an individual to receive a payment contingent on health status and then to allow the individual to deny access to the records needed to verify that

status. Second, where action has been taken in reliance on the authorization, the individual cannot revoke the authorization after the fact. A health information trustee who discloses protected health information relying on an authorization that has been revoked shall not be liable if the reliance was in good faith, the trustee had no notice of the revocation, and the disclosure was otherwise lawful.

There is a special provision for authorized disclosures pursuant to subpoena, warrant, or search warrant. In many instances, section 5140 requires notice to the individual before protected health information may be disclosed pursuant to a subpoena or warrant. If an individual consents to disclosure pursuant to a subpoena or warrant, then there is no reason to comply with the notice requirement. In this case, a trustee may disclose protected health information pursuant to an authorization and in response to a subpoena or warrant if the authorization specifically references the subpoena, warrant, or search warrant and if the authorization otherwise meets the requirements of the Part. Basically, it is acceptable for a trustee to comply with a warrant under circumstances where the individual has specifically consented to the disclosure pursuant to specified compulsory process.

In general, the Committee expects that execution of authorizations will become relatively rare events for most patients. Today, every insurance claim form contains an authorization of disclosure. These authorizations tend to be extremely broad. Their purpose is to permit maximum disclosure with minimum restriction and liability. They protect only the person who seeks the authorization and not the person who is authorizing the disclosure. Few patients are actually aware of the presence or scope of the authorizations. Even fewer are in a position to argue or amend any authorization, and a patient who seeks to make a change in the authorization risks losing insurance coverage altogether.

The Fair Health Information Practices Part lays out a different approach. Rather than rely on the fiction of informed consent for routine disclosures for treatment or payment, these disclosures are authorized in law under fair conditions that protect both patient and trustee. This approach avoids loopholes whereby information is provided to some with the consent of the individual, but the information loses any legal protections or restriction in the hands of the recipient. By using the Part's process for disclosure, information remains subject to restriction in the hands of the recipients because the statutorily designated recipients remain health information trustees. This same protection is not available today, and it cannot be fully realized under a system that relies solely on "informed" consent. The result is that patients received clearer, better, and more comprehensive protection for sensitive health information. Others who require health information to carry out their activities will be able to obtain the information in a simpler and less expensive manner because authorizations will no longer be needed for routine functions. The price for this convenience is a greater duty to protect the information that is obtained and legal liability for failure to use the information in accordance with the law. This is a workable, fair, and balanced approach that makes patients and trustees better off and reduces cost.

The Committee recognizes that there will be some individuals for whom the statutory authorizations for payment or treatment are troublesome. Traditionally, some individuals have sought health care in a manner that avoids disclosure to their insurance company or employer. For these patients, there is protection available under the Fair Health Information Practices Part. Section 5131(e) permits an individual to restrict use or disclosure of protected health information to a greater degree than would otherwise be required. Where an individual enters into a formal agreement with a trustee for such restrictions, the trustee is bound by the limitations and may be sued for failure to comply. Thus, a patient who insists on paying cash for care so that his insurer does not know about the treatment can avoid disclosure to the insurer pursuant to the provisions that permit disclosure to benefit plans. Section 5131(e) requires a formal agreement so that there is a clear record of the restrictions that both parties have negotiated.

Section 5193(c) includes a transition provision for an authorization for the disclosure of protected health information that was executed before the effective date. If the authorization is otherwise valid under state or applicable law won the effective date, that authorization remains valid for a year or until the date or event when it would otherwise expire, whichever comes first. During this transition period, valid, pre-existing authorizations do not have to meet the standards of section of 5132 for authorizations.

SECTION 5133. TREATMENT, PAYMENT, AND OVERSIGHT

Section 5133 establishes the basic rules and procedures that govern disclosures for treatment, payment, and oversight. The health information trustees who are eligible to make disclosures under this section are health benefit plan sponsors, health care providers, health oversight agencies, and health information service organizations. These trustees may disclose protected health information to a health benefit plan sponsor, health care provider, or health oversight agency for one of three authorized purposes.

First, disclosure may be made for the purpose of providing health care as long as a protected individual who is a subject of the information has not previously objected to the disclosure in writing. This permits a physician to consult with another physician about the treatment of a particular individual without the need for specific consent. In the overwhelming majority of circumstances, this type of consultation is unobjectionable. A patient who has a concern can, however, make a written objection, and the trustee is bound to heed the objection.

Disclosures are not limited to those that pertain to the treatment of the subject of the records. A disclosure for treatment can be made in connection with the treatment of any individual. For example, a physician in a hospital who is treating a patient with a rare disease may, in the absence of an objection, examine the records of other hospital patients with the same disease. However, obtaining access for treatment does not authorize the physician to disclose identifiable information about those other patients to the current patient. That type of disclosure would be not be authorized under this section or under any other section of the part.

Second, disclosures may be made for the purpose of providing for the payment for health care furnished to an individual. The authority to make these disclosures without the express consent of a patient is a key element of the new approach toward disclosure taken in the Fair Health Information Practices Part. See the earlier discussion about the shortcomings of informed consent.

Individuals with special concerns or who simply do not want these disclosures made without their express consent have the tools under the legislation to make alternate arrangements. In addition, the authority to make disclosures for payment is not unlimited. It remains subject to the general rule that disclosures must be limited to the minimum amount of information necessary to accomplish the purpose for which the disclosure is being made. This is a significant limitation. Under current practice, individuals are typically asked to sign consent forms that permit disclosure or any or all information. Under that authority, an insurance claim could include an entire medical record. Under the authority in section 5133, it will no longer be possible to disclose an entire record in connection with a claim for current treatment. Only the information necessary to process the claim can be disclosed. In this case, the provider has authority to disclose without express consent, but the provider also has responsibility to limit the disclosure.

SECTION 5134. NEXT OF KIN AND DIRECTORY INFORMATION

Section 5134 permits health information trustees who are health care providers or who received information pursuant to the emergency circumstances section may make disclosures to a patient's next of kin or of directory information. For each of these disclosures, there are strict limits on the type of information that can be disclosed and the circumstances of the disclosure.

Next of kin disclosures present some complex policy problems. Serious concerns have been expressed that physicians are sometimes insensitive to the confidentiality interests of patients and make disclosures to family members that the patients would not approve.[115] It is also true that physicians routinely share information with family members in a manner that enhances health care and that does not raise objections from patients. In most instances, physicians exercise discretion for these disclosures with care and appreciation for the interests of patients.

The next of kin issue was discussed at a hearing by Subcommittee Chairman Gary Condit and Dr. Donald T. Lewers, a practicing physician who testified on behalf of the American Medical Association.

> Mr. CONDIT. The bill gives doctors discretion to disclose some health information to a patient's next of kin. This reflects current practice where doctors exercise judgment about what to tell a patient's spouse, except where the patient has objected.
>
> This section has been quite controversial. Do we need to have a written authorization before a doctor can make a routine disclosure to a spouse?

---

[115] See, e.g, testimony of Aimee Berenson, Legislative counsel, AIDS Action Council; and Susan Jacobs, Staff Attorney, Legal Action Center, in H.R. 4077 Hearings (May 5, 1994).

Dr. LEWERS. This is a very difficult area. And I deal with it on a daily basis as a practicing physician. I think in general it is accepted, as you said, that we do release information to the next of kin, to the legal next of kin. The problem gets in where there is separation between spouses, and individuals who are not living with an individual who still legally is the next of kin, and sometimes that gets very hairy.

I've been in practice 25 years. I've only had two instances where an individual has come to me and said I do not want you to release information to my family, to my spouse, any information.

I get that in writing and document it and then hold it. And as a matter of fact have locked those records. But I don't see that as a big problem. It may be a larger problem as time goes on and perhaps we have more problems with social issues of separation, et cetera. But at this point, it's one we have been able to work with.

I'm not sure you need to try to get into that. That's going to be complex and difficult, I would think, to write. And it would make more of a hassle to sue in again making sure that we have that information; how often are you going to update it, et cetera.

Mr. CONDIT. So your response would be we do not need a written authorization?

Dr. LEWERS. My feeling is that we do not, at this point. I don't think it's much of a problem. We run into it every day, and I don't think you need to put it into law.[116]

In the context of comprehensive fair health information practices legislation, it is not possible to avoid the issue altogether. Providing statutory rules regulating next of kin disclosures is not a simple task. It is impossible to describe all of the circumstances that might justify these disclosures. The Committee recognizes the sensitivity of next of kin disclosures and has attempted to respond to the concerns without imposing legalistic or bureaucratic rules that will unduly interfere with the physician-patient relationship.

The legislation proposes to allow physicians limited discretion with respect to next of kin disclosures. Under the section, only health care providers are authorized to make next of kin disclosures. With one exception, other health care trustees are not authorized to disclose any information to a next of kin. The exception is for a trustee who obtains protected health information as a result of an emergency circumstance disclosure.

Disclosures may only be made under this provision orally. Providing access to written records is not within the scope of the section.

Disclosures can only be made to a patient's next of kin as defined under State law or to a person with whom the individual has a close personal relationship. It is not at all unusual that the principal caregiver to a patient may not be the legal next of kin. It may be a roommate or a distant relative. The physician will have to make a determination about who is a qualified recipient. Doubts

[116] H.R. 4077 Hearings (May 4, 1994).

should be resolved by asking the patient or by not making a disclosure.

There are four specific limitations on a physician's discretion to disclose to next of kin. First, if the patient has previously objected, then the physician cannot make a next of kin disclosure. The objection does not have to be in writing to be effective.

Second, the disclosure must be consistent with good medical or other professional practice. Thus, if it is the accepted practice of psychiatrists not to discuss any information about a patient with next of kin, then disclosures under this section would not be permitted.

Third, any disclosure must be limited to information about health care that is being provided to the individual at or about the time of the disclosure. Thus, for example, if a patient is being treated for a broken leg, a physician could discuss aspects of the treatment with the patient's spouse. But disclosure of information about previous types of treatment ("Did you know your wife had a drinking problem twenty years ago?") would be prohibited.

Finally, in order to further limit the possibility that a physician might misinterpret the discretion granted under the section, the Committee added another limitation. A physician can only make a disclosure if the physician has no reason to believe that the individual would consider the information especially sensitive. Thus, a physician treating a patient for a sexually transmitted disease, mental health problems, AIDS, or a similar problem would have to think twice before making any disclosure under the next of kin authority. For these types of ailments, the physician would have to be certain that the patient would not consider the information to be especially sensitive. It would not, however, prevent a physician from sharing information that the patient would not consider to be sensitive. Thus, even when the diagnosis is sensitive, it might be acceptable to inform a spouse that the patient should stay in bed or follow specific dietary requirements without disclosing the actual diagnosis.

Section 5134(b) authorizes the disclosure of directory information about a patient who is currently receiving health care from a health care provider or at premises controlled by a provider. Directory information includes only the name of the patient, the location (i.e., room number) of the patient on the premises, and the general health status of the patient. The description of general health status is limited to words like critical, poor, fair, stable, satisfactory, or similar terms. Directory information that is disclosable may be disclosed to any person.

There are additional limitations on the disclosure of directory information. First, a trustee may not disclose directory information about an individual if the individual has objected in writing. If an individual objects in whole or in part to the disclosure of directory information, that objection is binding on the trustee. Of course, an individual can agree to a disclosure of additional information, but the requirements for authorizations in section 5132 will have to be met.

Second, the disclosure of directory information must be consistent with good medical and other professional practice. Thus, if the practice for a psychiatric treatment facility has been never to dis-

close the name of patients, then that practice would prevent the disclosure under section 5134(b).

Third, any directory information disclosed may not reveal specific information about the physical or mental condition or functional status of a protected individual or about the health care provided to a protected individual. If a facility offers a single category of treatment (e.g., for addiction, mental health, etc.), then disclosing the name of patients would reveal information about their condition or treatment. If so, then directory information could not be disclosed without the consent of the patient.

Any information disclosed under section 5134 is not subject to the accounting requirements in section 5124 of the bill. There is no need to keep an accounting of the disclosure in these instances. Also, the recipients of information under section 5134 are not by reason of receiving the information subject to any of the requirements of the Fair Health Information Practices Part. As a result, an individual who is provided information about a spouse does not become a health information trustee. Some recipients of directory information may otherwise be health information trustees, and they remain fully subject to the provisions of the Part.

SECTION 5135. PUBLIC HEALTH

Health care providers and public health authorities are authorized in section 5135 to disclose protected health information in two circumstances. Disclosures may be made to a public health authority for use in legally authorized disease or injury reporting, public health surveillance, or public health investigations or interventions. This authorizes providers and others to disclose information for a variety of inquiries and interventions to protect the public health and safety.

Disclosures may be made for traditional public health surveillance, investigation, and intervention with respect to communicable disease as well as other conditions and injuries. In all States, certain conditions are required to be reported to public health authorities. The bill allows disclosures to comply with these requirements, including those imposed directly by statute and those imposed by administrative action based on statutory authority. While not all public health surveillance activities require identifiable information, many do. These programs are especially important in management and control of infectious disease.[117] This section also permits other disclosures to public health authorities that are necessary for investigation or intervention, such as identifying all the persons who might have been exposed to a person with a communicable disease.

Public health agencies that receive information are sharply constrained in how they may further disclose it in identifiable form. Public health authorities have a long ethical tradition of complete

[117] Infectious disease is still a serious threat to health. See, e.g., Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, "Addressing Emerging Infectious Disease Threats: A Prevention Strategy for the United States" (1994). In this report, a major objective offered by CDC is expansion and coordination of surveillance systems for the early detection, tracking, and evaluation of emerging infections in the United States. The report states that "[s]urveillance is the single most important tool for identifying infectious diseases that are emerging, are causing serious public health problems, or are diminishing in importance." Id. at 12.

confidentiality in the conduct of their investigations, and are subject to confidentiality obligations under State law. They carefully safeguard information. However, there may be instances where their inquiries may involve implicit or explicit disclosures of patient identities in order to conduct their investigations and interventions, and such disclosures are not forbidden, as long as they are in accordance with State law and are necessary for a public health purpose. This provision permits, for example, spousal notification programs.

Information received by a public health authority under this section may not be used or disclosed in any administrative, civil, or criminal action or investigation directed against the patient, except where the use or disclosure is authorized by law for the protection of the public health. This generally prohibits all collateral uses of patient information, except in actions like proceedings to isolate or quarantine a person with a communicable disease—such as tuberculosis—who endangers the public health.[118]

This section is also a basis for certain disclosures to private entities, operating under legal authority, in the course of public health surveillance and similar activities. The definition of public health authority in section 5120(b)(9) includes a person acting under the direction of a public health authority. Similarly, cancer registries[119] are sometimes operated by non-governmental research institutions, and reports to them are required by State law as part of a program to identify the causes of cancer. The tracking of medical devices, required by the Federal Food, Drug, and Cosmetic Act[120], may require that patient identifiers in some instances be reported by physicians to device manufacturers.

An individual who receives information pursuant to the disclosure authority for public health interventions does not become a health information trustee and is not subject to any requirement as a result. If a disclosure is made under this authority to a health care provider or other person who is otherwise a health information trustee, this does not exempt that trustee from its obligations under the part. The policy is directed at spousal notification where the imposition of confidentiality duties would not make sense or be effective.

SECTION 5136. HEALTH RESEARCH

Section 5136 establishes rules for disclosure of protected health information to health researchers. The importance of health research to the Nation's health and well-being can be illustrated in many different ways. One can point to the dramatic increase in the life expectancy of Americans, the list of diseases that are no longer serious threats to health, or to the billions of dollars appropriated each year by Congress to support research. Health research is an integral and necessary part of the modern health care system, and

[118] The emergence of multidrug resistant tuberculosis has renewed attention to the powers of States to isolate and quarantine individuals who endanger public health. All States have laws to assist in controlling the spread of communicable diseases. See Gostin, "Controlling the Resurgent Tuberculosis Epidemic", 269 Journal of the American Medical Association 255 (1993).

[119] See, e.g., §§ 399H–399L of the Public Health Service Act, 42 U.S.C.A. §§ 280e–280e4 (West Supp. 1994).

[120] 21 U.S.C.A. 360i (West Supp. 1994).

access to health care records is vital to the conduct of some health research projects.

Researchers point out that it is impossible to carry out many types of research without access to identifiable patient records. In testimony delivered on behalf of the Society of Epidemiological Research and the Association of American Medical Colleges during consideration of a similar bill during the 96th Congress in 1979, Dr. Leon Gordis, Chairman of the Department of Epidemiology at the Johns Hopkins School of Hygiene and Public Health offered several specific examples of epidemiological studies that could not have been conducted without access to identifiable medical records:

A. DES AND VAGINAL CANCER

In order to convey some idea of just how important the legitimate research use of medical records is, I should like to cite a few major findings from several epidemiologic studies. First, I should like refer to the studies dealing with diethylstilbestrol or DES as it is known. These studies of the effects of DES in human beings are particularly important since for many years DES was added to livestock feeds in the United States. A few years ago, investigators in Boston demonstrated through an epidemiologic study, that when mothers took DES during pregnancy to prevent a miscarriage, female offspring of these pregnancies were at increased risk of developing a rare type of cancer of the vagina when they reached adolescence.

This study could only have been carried out through the use of medical records. Three particular features are noteworthy here: First, the cancer did not appear in the person taking the medication but only in her female offspring exposed to DES during intrauterine life. Second, the cancer appeared some 15 to 20 years after exposure to DES so that it was necessary to go back many years to determine exposures and to identify the drugs taken in pregnancy. Third, in this study, the girls and young women who had this cancer were first identified from their medical records, and only then could their mothers be contacted and followed-up. Consequently, if use of medical records were prohibited, or if such use were permitted only with the consent of the patient, these studies which demonstrated the cancer-producing effect of DES in women many years after exposure, would have been impossible to carry out.

This study is perhaps the first demonstration in human beings of transplacental carcinogenesis, i.e., that cancer causing agents taken by the mother can cross the placenta and produce cancer in the offspring. There may be other such agents—presently unknown—which mothers should avoid during pregnancy because of the hazard to their children. In order to identify these agents, thorough epidemiologic investigations using medical records are needed to protect the health of American women and their children. This is an area which could not be explored, however, if restrictions were placed in research uses of medical records.

B. OCCUPATIONAL CANCERS

I should like to turn to another important area—the health of the American worker. In recent years, there has been increasing recognition that Americans employed in industries are often subjected to high concentrations of potentially toxic substances. Thus, for example, workers exposed to vinyl chloride have been shown to be at high risk of liver cancer. This finding, which has now been confirmed in a number of studies, could only be made by reviewing the medical records of large groups of employees in specific industries and linking the employees' records at the factory site with hospital records and death certificates if they exist. Without access to these records it would be impossible to have identified vinyl chloride as a cause of cancer in occupationally exposed human beings. I should also point out in this connection, that if there were a requirement that patient consent be obtained before the records were made available—these studies could also not have been carried out because many patients had either died by the time the study was done or else had moved and could not be traced.

It is clear that we have only begun to scratch the surface in terms of the toxic and cancer-producing potentials of substances to which American workers are exposed in the course of their daily labors. Any restriction which would preclude the possibility of identifying new damaging substances and documenting their harmful effects would be a major setback to the protection of the health of the American worker.

C. PREVENTIVE BLINDNESS IN PREMATURE INFANTS

I should like to turn briefly to a tragic medical story which unfolded during the 1950's. At the time premature infants who were of low birth weight, were found to have an increased risk of a form of blindness called retrolental fibroplasia. Surprisingly, the risk of blindness was highest in the best medical centers in our country while in the less sophisticated and less well-equipped medical centers, the risk seemed lower. Initially there was no clue as to what might be causing this blindness and numerous investigations in many areas were carried out. However, epidemiologic investigations subsequently demonstrated that the cause of this blindness was high oxygen concentrations administered to the premature newborns. These high concentrations were often only provided in the best medical centers, since at that time, the highest possible oxygen concentration was considered the best medical care for these infants. Since that time, restriction of the oxygen concentration to a lower level when administered to premature infants has virtually wiped out this form of blindness in prematures. Again, these studies which demonstrated that high oxygen concentrations were the cause of blindness in children and that reducing these concentra-

tions could prevent such blindness, would have been totally impossible to carry out were access to medical records restricted.

D. BENEFITS OF ANTICOAGULANT DRUGS FOR PATIENTS WITH HEART ATTACKS

For many years, there has been a difference of opinion among physicians with regard to the possible effects of anticoagulants in the treatment of patients who have heart attacks. Several years ago, we carried out a study in which we reviewed the records of a large number of patients who had heart attacks and who had been hospitalized some years previously. We ascertained which patients had received anticoagulants and which patients had not, and then determined which patients had died during their hospitalizations. We were able to show that the death rate was much lower in patients who had received anticoagulants during their hospitalization than in those who had not. This important observation has now been confirmed in another study carried out in our Department. We believe that in the coming years, these findings will have major implications for care of heart attack victims. Yet both studies could not have been carried out without the use of medical records and identifying information, and would have been impossible had the consent of the patient been required for reviewing these records.

E. HARMFUL EFFECTS OF THE PILL (ORAL CONTRACEPTIVES)

Although the "pill" has been demonstrated to be a highly effective and convenient form of birth control which has been adopted by many American women as their form of contraception, a large number of epidemiologic studies have now demonstrated that women taking the pill for long periods of time are at an increased risk for blood clots, strokes, heart attacks, high blood pressure, liver tumors, gallbladder disease, congenital malformations in their offspring and other conditions. These highly significant findings were in large measure the result of large scale studies which used hospital and medical records—studies which again would have been impossible to carry out if patient consent had been required.

F. IMPROVED SURVIVAL OF CHILDREN WITH LEUKEMIA

One of the greatest accomplishments of American medicine during the past two decades has been the breakthrough in the treatment of acute leukemia in children. While children with leukemia at one time died within a few months after diagnosis, with the new advances in therapy, they now live many years—and are often free of any evidence of their disease. The demonstration that new forms of therapy have resulted in an improved outcome

such as this for the patient also requires the use of medical records.[121]

Statistical projects, health services research, and health related behavioral research also depend upon access to identifiable patient records in order to be effective.[122] Reporting systems and surveys of hospital care, physicians' services, nursing home care, and other institutional and home care provide information on access to health care, indicators of quality and cost of care, and data showing variations over time.

Research on health encompasses many factors beyond the facts elicited through medical diagnosis and evaluation. Thus, the definition of allowable research for which disclosures may be made includes "behavioral and social factors affecting health." Health research often includes the study of social and behavioral factors that influence health outcomes. For example, family composition, age, income, labor force participation, and area of residence all influence health conditions and are useful in planning and evaluating the effectiveness of health care delivery and in setting policy with regard to health programs. Health care data may also be used indirectly in health statistics and research activity. For example, enrollment data in the health care program could be used for improving our understanding of the population in general statistical activities, the results of which can be used by health researchers and policy makers to understand health outcomes.

If researchers had to obtain specific patient consent before records could be used, many research projects would never be undertaken. There are several reasons why patient consent is an impractical requirement. Many studies are initiated after the original health care information was recorded. It would be impossible to foresee all possible studies for which a health care record might be valuable and to obtain consent in advance. Few if any patients have ever been asked to sign such consents, and most existing records would not be available to researchers.

It might therefore be necessary to obtain specific consent for each proposed research project. However, review of patient records by researchers is frequently the first step in identifying patients with the disease that is to be studied. Until the records are reviewed, the patients cannot be identified to ask for consent. Yet if the consent were required, the patients could not be asked to give consent until they were identified by looking at the records. This is clearly an impossible situation.[123]

There is another aspect of patient consent that makes it a poor prerequisite for research. The unavailability of or lack of consent from some patients could seriously bias the results of the research in an unforeseen way. The exclusion of some records from a study

---

[121] "1979 House Hearings" at 484-89.

[122] For a discussion of the Administration's plans for health research activities, see testimony of Nan D. Hunter, Deputy General Counsel, Department of Health and Human Services, in "H.R. 4077 Hearings" (April 20, 1994). For a discussion of the use of health records in statistical activities, see the statement submitted by Norman Bradburn, Chair, Committee on National Statistics, National Research Council, in "H.R. 4077 Hearings." See also Committee on National Statistics, "Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics" (1993) (National Research Council).

[123] 1979 House Hearings at 483-4 (testimony of Dr. Leon Gordis, Society for Epidemiologic Research and the Association of American Medical Colleges).

might not happen in a random fashion. Patients with a certain significant medical feature might tend to be the patients who refused consent. The consequence of permitting some records to be excluded from a study is to raise doubts about the validity of the study.

Section 5136 strikes a fair balance between the confidentiality interests of patients and the needs of health researchers. Most health information trustees may disclose protected health information for health research. Section 5136(d) identifies the trustees who may not make disclosures for research purposes. Those who become health information trustees because of disclosures under section 5138 (relating to judicial and administrative purposes), paragraphs (1), (2), or (3) of section 5139(a) (relating to law enforcement), or section 5140 (relating to subpoenas, warrants, and search warrants) may not disclose information to health researchers.

All other trustees may disclose protected health information to health researchers subject to three general conditions. First, the disclosure must be to a person who is conducting an approved health research project. An approved health research project is defined in section 5120(c)(3) to be a biomedical, epidemiological, or health services research or statistics project, or a research project on behavioral and social factors affecting health, that has been approved by a certified institutional review board (IRB). The definition of the type of research that can qualify as a health research project is intentionally broad. Limitations are best imposed by the IRBs rather than by a restrictive and inflexible statutory definition.

Second, the protected health information to be disclosed must be used in the health research project. There is no need to disclose information that will not be used in a research project.

Third, the health research project must have been determined by a certified IRB to be of sufficient importance so as to outweigh the intrusion into the privacy of the protected individual who is the subject of the information that would result from the disclosure. This is obviously a balancing test. Any disclosure of protected health information involves an invasion of privacy. Where there are appropriate protections for the information, the risk of further invasions of privacy is small. Nevertheless, the consequences of the disclosure for patient privacy must be weighed against the importance of the research, its probable value to society, and the likelihood of success.

No specific guidelines for making this judgement have been included in the bill. Institutional review boards are already in existence and are already making similar evaluations. The decision about privacy should be made in the same fashion, relying on the knowledge and experience of the members of the board. The Secretary can provide additional guidance as appropriate through the regulations that will implement the certification requirement for IRBs that is contained in section 5136(e).

There is a second test that IRBs must apply when evaluating health research projects. The IRBs must find that it is impracticable to conduct the research without the information. This does not mean that it must be impossible to conduct the research in any other way, nor does it require that patient consent be obtained if at all possible. The IRBs may weigh such factors as cost, time and

other resources available for data collection, and the quality of results. Of course, when an alternative to the disclosure of identifiers would not be unreasonably disruptive to the research, the IRB could require use of that alternative.

There are several conditions that attach when protected health information is disclosed for use in a health research project. First, the health researcher may only use the information for the purposes of an approved health research project. Any other use would be a violation of law and would subject the researcher to criminal or civil penalties as applicable. A researcher would want to use or disclose protected health information for a purpose not originally approved by an IRB must return and receive permission from the IRB prior to any other use or disclosure.

Second, the health researcher may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the subject of the protected health information. If a patient's information is to be used for research, it is fair and appropriate that the patient not be jeopardized as a result of that use. Information that a patient told a physician in confidence that is subsequently made available to a health researcher may never be used against the patient in any way. This absolute protection is an essential part of the bargain that permits use of records by researchers.

Third, the researcher must remove or destroy information that would permit individuals to be identified at the earliest opportunity consistent with the purpose of the project, unless an IRB has determined that there is an adequate health or research justification for retention of identifiers and that there is an adequate plan to protect the identifiers from any use and disclosure that is inconsistent with the Fair Health Information Practices Part. A health researcher who wants to retain identifiers must apply to a review board for permission. This may be done at the time that a project is approved initially or at a later time.

There are several reasons why it may be important to permit the retention of identifiers after a study has been completed. First, when results are published and reviewed by other researchers and by scholars, questions about the conduct of the research or the accuracy of the data may arise. If the identifiers have been destroyed, the may be no way to verify the results and the validity of the research will be in doubt. There have been enough cases of fraudulent research in recent years to make this a serious concern.

Second, it is possible that the results of one study when combined with the results of concurrent or subsequent studies may suggest new lines of analysis. Early destruction of identifiers may make it impossible to reanalyze or recombine data or consider new hypotheses.

Third, even when there is no immediate need for identifiers after a study is complete, the possibility that a follow-up study may be done in the future may provide a sufficient reason for retention. If identifiers are destroyed, future avenues of research may be arbitrarily cut off, and money or time may be wasted duplicating the original research. For example, if the effect of a new drug or medical technique is studied and the identifiers are destroyed upon completion, it may not possible to reopen the study five or ten years

later to investigate the possibility of additional and unforeseen side effects. Other long range studies of specific populations may also be prevented.

For these and similar reasons, automatic destruction of identifiers is not required. Where a researcher wants to retain identifiers beyond the immediate needs of the research project, the researcher must obtain specific approval from an IRB. The standard established in the bill—an adequate health or research justification for retention—is intentionally liberal. If there is a reasonable likelihood that the identifiers might be valuable in the future, an IRB may approve retention.

Any long-term retention of identifiable data entails additional responsibilities on the part of the researcher for the protection of patients. In order to assure that the identifiers will not be misused or improperly disclosed, the researcher must present the institutional review board with an adequate plan for the protection of identifiers. The plan should provide for the storage of identifiers in a reasonably safe place under the custody of a person who is aware of the sensitive nature of the information and of the procedures that must be followed before any further disclosure is permitted. Disclosure of protected health information by one researcher to another can only be made with the approval of an institutional review board.

The identifiers may be left in the custody of the researcher, the institutional review board, or other responsible person or institution. Security plans do not have to be unnecessarily elaborate or expensive, and identifiers need only be provided with a reasonable degree of protection given the potential threats to misuse. The institutional review board must approve the plan of the researchers, but it is the researcher who is responsible for carrying out the plan as approved.

For some types of research projects, the need for long-term or permanent retention of identifiable patient information is a necessary feature of the project itself. In the case of registries, such as tumor, cancer, or other diseases, one purpose of the project is the creation of an information resource for the use of other researchers.[124] Approval for identifier retention for registries should present no difficulties for an institutional review board.

Section 5136(e) describes the general requirements for certification of IRBs by the Secretary of HHS. The certification process will give the Secretary the ability to exercise both substantive and procedural control over the activities of IRBs. Independent oversight of IRBs is important. The Working Group on Ethical, Legal, and Social Implications of the Human Genome Project points out that IRBs are not independent of the institutions that created them. The inherent conflict of interest is particularly strong when an IRB reviews research with commercial potential for the institution or company at which the IRB is located. These conflicts are less likely to be present when an IRB reviews research sponsored

[124] Disease registries can qualify as health research projects and can receive protected health information as long as their activities have been approved by an IRB. In the case of registries operated by or at the direction of public health authorities, IRB approval may not be necessary. Section 5135 authorizing disclosures for public health permits disclosures to public health authorities for disease or injury reporting and for public health surveillance.

by another institution. The Secretary may issue rules covering situations where there is an inherent conflict of interest.

The certification requirement is not intended to produce a major change in existing IRBs, and the bill requires that the regulations be based on existing IRB rules under section 491(a) of the Public Health Service Act. There may be a need for different rules for IRBs that review commercially sponsored research or for IRBs that make determinations regarding disclosure of information from health information service organizations.

SECTION 5137. EMERGENCY CIRCUMSTANCES

Section 5137 authorizes all health information trustees to make disclosures of patient information in emergency circumstances. The specific requirements are that the trustee must believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual. A common circumstance will be when an individual is brought into an emergency room, and records of previous treatment are needed to assist in providing immediate health care. The authority is not limited, however, to disclosures for the treatment of the subject of the information. Another circumstance might involve the disclosure of psychiatric information about a person holding a hostage who poses a serious and imminent threat to the safety of the hostage.

The language in the bill was drawn from a similar provision in the New Zealand Health Information Privacy Code 1994 issued by Bruce Slane, the Privacy Commissioner of New Zealand.[125] Mr. Slane also provided an excellent illustration of the application of the policy for emergency disclosures using an older court decision involving disciplinary proceedings against a physician for breach of confidence.[126]

The facts of the case were that Dr. Duncan was a medical practitioner in a rural community. Mr. Henry, a patient of Dr. Duncan's and a bus driver by occupation, had a series of heart ailments. On the day before Mr. Henry was to drive on a charter trip, Dr. Duncan spoke to a woman who was to be a passenger and advised her that Mr. Henry was not fit to drive. Dr. Duncan also spoke to Mr. Henry and to the police constable. Dr. Duncan also asked a patient to help organize a petition to have Mr. Henry barred from driving passenger vehicles. Following a complaint, a professional disciplinary committee found Duncan guilty of misconduct for breach of professional confidence. It was the disclosure of information to lay people—and not to the constable—that was the cause for the censure.

Privacy Commissioner Slane applied the facts of this case to the emergency disclosure provision in the New Zealand code. He found that first, Dr. Duncan would need to believe on reasonable grounds that it was not desirable or practicable to get Mr. Henry's authorization for the disclosure. Second, Dr. Duncan would need to believe on reasonable grounds that (i) there is a serious threat to public safety; (ii) the threat was imminent; (iii) the disclosure of

[125] Rule 11 (2)(b).

[126] The discussion of the *Duncan* case comes from a speech given by Mr. Slane at the Wellington (NZ) School of Medicine on February 9, 1994.

the information to the constable would prevent or lessen the threat; and (iv) the disclosure of Mr. Henry's medical information was necessary to prevent or lessen the threat (that is, the threat could not be prevented or lessened in some other way not involving a beach of confidence). Third, the disclosure made to the constable would have to be limited to the information necessary to prevent or lessen the threat to public safety. This means that disclosure to persons other than the constable was unnecessary. Mr. Slane concluded that disclosure to the constable was probably acceptable, although a road licensing authority might have been a better choice. Mr. Slane also suggested that disclosure to the potential passenger might be justified, although his remarks are not definitive on this point.

Privacy Commissioner Slane's analysis is generally instructive for the provision in the Part. The last point raises a highly controversial matter in this country that involves the physician's duty to warn. The leading case in the United States is *Tarasoff* v. *Regents of the University of California.*[127] In that case, a psychologist was told by a patient that the patient intended to kill a third person. The psychologist notified the police but did not warn the intended victim. The patient subsequently killed that person. The Supreme Court of California found that the therapist had an obligation to use reasonable care to protect the intended victim against danger, including warning the victim of the peril.

The *Tarasoff* decision has been controversial, and not all states have reached the same conclusion. Regardless, the emergency disclosure provision in the legislation takes no substantive position on a trustee's duty to warn. If such a disclosure is required or appropriate under applicable law, then it may be made consistently with the Fair Health Information Practices Part. However, there is no requirement that a disclosure that is authorized must be made by a trustee. If a duty-to-warn disclosure is not required or appropriate under state or other applicable law, then there is no obligation section 5137 to make the disclosure. The Fair Health Information Practices Part is completely neutral on the substantive question, but it permits a duty-to-warn disclosure provided that the standards for emergency disclosures are met.

It is much more likely that the emergency disclosure authority will be use to assist in a treatment setting. Robert Bolan, Vice Chairman of the Board of Directors of Medic Alert Foundation testified about the problems and the promise of requests for emergency disclosure of medical information:

> Medic Alert is currently the largest information data bank of patient-supplied medical information in the world. It has been estimated that Medic Alert helped avert tragedy in over 207,000 medical emergencies since the Foundation's inception. Speed of delivery is crucial for emergency treatment. The emergency room or trauma scene is a diagnostic epicenter where lives are won or lost by seconds. Emergency physicians and paramedics walk a tightrope between protecting a patient's right to privacy and accessing private medical information when he or she is

[127] 17 Cal. 2d 425 (1976).

> unable to authorize disclosure. Medic Alert has grappled with this privacy issue since 1956 and although 100-percent confidentiality cannot be guaranteed, we will always err on the side of saving a life.[128]

The Committee recognizes the pressures and uncertainties that may arise when disclosures are requested under emergency circumstances. Decisions about disclosure must often be made instantaneously and without the ability to seek consent or to perform complete verification of the request. The language of the emergency disclosure section has been written with this in mind. The health information trustee can disclose protected health information under the emergency circumstances specified in the bill when the trustee believes on reasonable grounds that there is a need. A trustee who acts in good faith and makes a reasonable judgment cannot be liable if later events reveal that the judgment was in error. The trustee's judgment must be assessed for its reasonableness based on the information that was available to the trustee at the time the disclosure was made.

Information about an individual that is disclosed under the emergency circumstances section may not be used in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and related to health care or payment for health care. This is to protect an individual when information may be disclosed to law enforcement officials in an emergency. It is not intended to prevent some who receives a *Tarasoff* warning from seeking appropriate protection from the courts. Nor is the same information that has been disclosed otherwise protected from use for that purpose by the original trustee.

SECTION 5138. JUDICIAL AND ADMINISTRATIVE PURPOSES

Section 5138 authorizes three types of disclosures for judicial and administrative purposes that can be made by health benefit plan sponsors, health care providers, health oversight agencies, or by trustees who have obtained protected health information pursuant to section 5137 (emergency circumstances), or section 5140 (subpoenas, warrants, and search warrants).

Two of the disclosures are relatively uncomplicated. Disclosure may be made when directed by a court in connection with a court-ordered examination of an individual. The court can direct how the information is to be used to accomplish the purpose of the examination. Disclosures may also be made to assist in the identification of a dead individual. This might entail the use of dental or other records that may be needed in the identification process. Section 5138(b)(2) requires that the trustee be provided with written statement that the information is sought to assist in the identification of a dead individual.

The third type of disclosure is pursuant to the Federal Rules of Civil or Criminal Procedure or comparable rules of other courts or administrative agencies in connection with litigation or proceedings to which a protected individual who is a subject of the information and in which the individual has placed his or her physical or men-

[128] H.R. 4077 Hearings (May 4, 1994).

tal condition or functional status in issue. In this type of litigation or proceeding, the individual's privacy interest is necessarily more limited and, at the same time, the individual is already in a position to seek appropriate restrictions from the court.

Section 5138(b) sets out a process that will provide appropriate assurance to trustees as well as adequate notice to the protected individual. A person seeking protected health information pursuant to the discovery provision is required to notify the protected individual or the individual's attorney of the request for information. The person seeking the information must also provide the trustee in possession of the information with a signed document attesting 1) that the subject of the record is a party to the litigation; 2) that the individual has placed his or her physical or mental condition or functional status in issue; and 3) the date on which the subject of the record was notified of the request. The person seeking the information may not accept it from the trustee until ten days after the notice was given to the subject of the record.

This procedure will assure that there is actual notice to the subject of protected health information so that the subject will have an opportunity to object in a timely fashion. Just because there is litigation that involves an individual's medical information, it does not mean that the individual's entire medical file is necessarily relevant to that litigation. If there is a dispute, this procedure will allow it to be resolved by the tribunal considering the matter. The general rule in section 5131(c)(1) that disclosures must be limited to the minimum amount of information necessary to accomplish the purpose for which the information is to be used is fully applicable, and this rule may be used by patients to contest the scope of discovery requests.

In these matters, the trustee is generally in the position of a stakeholder. It may or may not have an independent interest to assert, but the procedure will allow the trustee to assert any such interest. The burden of assuring compliance with the patient notice requirement falls on the requester and not on the trustee. The requester cannot accept any of the information until the ten day notice period has elapsed.

Any information that is disclosed under section 5138 is subject to a very strict limitation on further use and disclosure. The information can only be used to accomplish the purpose for which the disclosure was made. This is appropriate because a person who succeeds in obtaining protected health information for a very specific purpose should not have unlimited ability to redisclose the information. The information may be used in the course of litigation—subject to any protective orders or restrictions imposed by the court—but collateral uses and disclosures are prohibited. A litigant who obtains information under section 5138 becomes a health information trustee and must comply with applicable provisions of the Fair Health Information Practices Part.

SECTION 5139. LAW ENFORCEMENT

Most needs of law enforcement agencies for protected health information can be satisfied through the use of compulsory process. Before protected health information can be obtained from a health information trustee, however, the agency must usually serve a copy

of the process upon the patient, who may challenge it in court. There are several circumstances under which notice to the patient is either unnecessary or would prevent the acquisition of medical information by police in a timely fashion. Section 5139 recognizes three types of disclosures of protected health information that any trustee (other than a health information service organization) may make to a law enforcement agency without the consent of the patient and without advance notice to the patient.

The first is when medical information is needed for use in an investigation or prosecution of a health information trustee. Health care fraud has become a large problem, and governments at all levels are making major efforts to combat it. The costs of fraud are very large and any significant interference with fraud investigations will only lead to further increases in cost.

Most investigations of fraud are directed at doctors or institutional care providers, and it is rare for a patient to be a target. Fraud investigation frequently requires large numbers of patient records in order to establish patterns of illegal activity. Notice to all patients whose records are inspected would not only be administratively burdensome, but would also be unsettling to patients. If every patient of a particular doctor or clinic received a notice about an impending investigation, many would become unduly alarmed and might unfairly conclude that their doctor was involved in criminal activity. Such a notice might also disrupt important medical treatment. On balance, it is better to allow for access for this important law enforcement purpose without notice to the patient. The other provisions of section 5139 described below offer adequate protection for the privacy rights of patients.

The second type of disclosure that is permitted under section 5139 is in connection with criminal activity committed against a trustee or an affiliated person of the trustee or on premises controlled by the trustee. This permits a trustee to report to the police that a crime has been committed by a patient on the premises of the trustee. Also, when a patient threatens or harms a trustee employee regardless of the location, disclosures are likewise permitted. This is normal reporting of criminal activity that might be made by any person who witnesses or is a victim of a crime. An example is where an inpatient criminally assaults another inpatient. Even though the information about the assault will be part of the medical information maintained by the trustee, the information may be reported to the police. Nothing in section 5139 prevents a trustee from reporting criminal activity committed by employees or visitors.

Information about totally unrelated criminal activity that a patient confides in his physician is not disclosable under this section. An example is where a patient in the course of treatment informs his physician of illegal narcotics activity. It is not a physician's role to report such information to the police. Of course, if a physician learns of activity that involves a threat to the life or physical safety of an individual, it may be appropriate for the physician to report the information. This type of disclosure is permitted under the emergency provisions of section 5137. However, under other less

compelling circumstances, communications between a patient and a physician should remain confidential.[129]

Finally, medical information may be disclosed if it is needed to determine whether a crime has been committed by a person other than the patient or the nature of such crime. This provision is intended to permit information about the victim of a crime to be made available in a timely fashion in order to allow police to fully investigate a crime or to allow prosecutors to determine the proper charge. For some crimes, the severity of the victim's injuries will be the determining factor in making a formal legal charge against a suspect. For medical information to be relevant, the crime will normally involve bodily injury to the patient.

As with all other disclosures that are permitted to be made without the consent of the patient, no trustee is required to make a disclosure except where compelled by another law. A request by police for information that may be disclosed under section 5139 is not compulsory unless some other law makes the disclosure mandatory. Trustees may exercise discretion in deciding whether the information that the police have requested should be disclosed.

Any disclosures for identification or location purposes are limited to information needed for such purposes. When police are attempting to locate an individual, there is no need for a trustee to disclose any protected health information other than an address and perhaps other relevant identification information. Confidential communications, diagnoses, and other specific information cannot be disclosed.

Another category of disclosure to law enforcement authority is permitted for a narrower class of health information trustees. All trustees other than health information service organizations, public health authorities, and health researchers may disclose information to assist in the identification or location of a victim, fugitive, or witness in a law enforcement inquiry. There are two basic circumstances under which this type of disclosure might occur. The first is when an identified suspect, fugitive, or witness is being sought by the police. A trustee may respond to an inquiry about the present whereabouts of such an individual. A hospital cannot be permitted to become a sanctuary for criminals or others wanted by law enforcement agencies. A patient's objection to the disclosure of his presence under section 5134 is not effective under section 5139 as to law enforcement agencies.

In order for a law enforcement agency to obtain information under the provisions described above, the agency must provide the trustee with a written certification signed by a supervisory official of a rank designated by the head of the agency specifying the information requested and stating that the information is needed for a lawful purpose under this section. A request that asks for all information in a medical record will not in all circumstances satisfy the requirement that the request be specific.

There are two other provisions that authorize disclosure to law enforcement agencies. Section 5139(b)(2) and (b)(3) permits health care providers and selected other trustees to comply with laws that

[129] Section 5194(f)(2) expressly preserves any law that requires the reporting of abuse or neglect information, and these laws will be an exception to the general rule in section 5139.

require the reporting of specific health care information to law enforcement authorities. This covers gunshot wound reporting laws and similar statutes. Subsection (b)(3) permits federal facilities to comply with these laws even though they may not legally required to do so.

Protected health information disclosed under this section may not be used in any administrative, civil, or criminal action or investigation against the patient except one arising out of and directly relating to the action or investigation for which the information was obtained. This limitation does not prevent use of information obtained under this section about a patient who is involved either alone or with his doctor in fraudulent activity against the health program being investigated. Information obtained under section 5139 may not be otherwise used or disclosed by the agency unless the disclosure is necessary to fulfill the purpose for which the information was obtained and is not otherwise prohibited by law.

SECTION 5140. SUBPOENAS, WARRANTS, AND SEARCH WARRANTS

Compliance by health information trustees with subpoenas, summonses, warrants, and search warrants is provided for section 5140. The section does not give a trustee new authority to refuse to comply with valid legal process, but it does establish some prerequisites for those seeking information by legal process and some limitations on the use of information so obtained.

For most types of legal process, specific access procedures (including patient notice and challenge rights) are set out in section 5151 and 5153. These procedures are described elsewhere in this report. In general, a person seeking protected health information from a health information trustee by legal process must provide the trustee with written certification that the applicable access procedures have been followed. The certification notifies the trustee that it may comply with the process without liability under the Fair Health Information Practices Part. Any person who certifies falsely may be subject to civil or criminal penalties.

Section 5140(a)(3) makes clear that patient notification and related requirements do not apply if there is a basis in a disclosure section of the Part for disclosing patient information, as long as the conditions in that section authorizing the disclosure are met. In these instances, the requirements of the other sections authorizing the disclosure provide safeguards for the individuals. Notice to individuals simply because compulsory process was being used, would serve no useful purpose, and might wrongly convey the impression that the patient was somehow being investigated.

For example, trustees can disclose protected health information to health oversight agencies under section 5133, pursuant to the conditions specified in that section. An oversight agency may have subpoena authority to compel disclosure by a trustee. For example, Inspectors General have such authority in the Inspector General Act of 1978.[130] Likewise, providers and others may disclose information to public health agencies for the investigation of disease or other health and safety hazards under section 5135. In many States, public health agencies have subpoena or warrant authority

[130] See 5 U.S.C. App. §6(a)(4) (1988).

to obtain information. Should a public health agency have to use that authority, the bill does not require that the public health agency comply with the access and challenge procedures under section 5153, as long as the request complies with section 5135.

The National Transportation Safety Board conducts investigations of certain accidents (such as airplane and train crashes), in an effort to improve the public health and safety by making recommendations for safety improvements, and it uses medical records in its investigations. It has authority to subpoena records.[131] Since its use of the subpoena authority would be in the course of a public health investigation, with disclosure authorized under section 5135, notification to the individuals would not be necessary.

The Occupational Safety and Health Administration and the National Institute for Occupational Safety and Health have authority to compel disclosure of health records for their public health investigations and occupational health research,[132] and the Mine Safety and Health Administration[133] has similar authority. If inquiries under these authorities qualify as public health investigations and comply with section 5135, or qualify as research and comply with the requirements of 5136, the individual notification provisions of sections 5151 through 5153 are not applicable if the agencies utilize their subpoena authority.

Any person obtaining protected health information through legal process in accordance with section 5140 becomes a health information trustee and is subject to the general requirements of the Fair Health Information Practices Part. A person who so obtains protected health information may not use or disclose the information in any administrative, civil, or criminal action or investigation directed against the individual, except an action or investigation arising out of and directly related to the inquiry for which the information was obtained.

There are special rules governing use of protected health information by grand juries. The restrictions on grand jury subpoenas originated with recommendations of the Privacy Protection Study Commission. The Commission's report[134] includes a brief history of the origin and use of grand juries and this observation:

> In essence, the Grand Jury subpoena *duces tecum* has become little more than an administrative tool, its connection with the traditional functions of the Grand Jury attenuated at best. One might characterize its current use as a device employed by investigators to circumvent the stringent requirements which must be met to obtain a search warrant. Documents are subpoenaed without the knowledge, not to mention approval, of the Grand Jury. Documents summoned in the Grand Jury's name may never be presented to it. Indeed, the evidence obtained may not even reach an attorney for the government; it may simply be examined and retained by investigative agents for unspecified future uses. The unique powers of inquiry and

[131] 49 U.S.C. § 1903 (1988).
[132] 29 U.S.C. §§ 657, 669 (1988).
[133] 30 U.S.C. § 813 (1988).
[134] PPSC Report.

compulsion, theoretically justified by the secrecy and limited effect of Grand Jury deliberations, have become a generalized resource for Federal investigative activities.[135]

A similar conclusion was reached in a recent decision by the Court of Appeals for the First District of Texas.[136] In a concurring opinion, all three judges who decided the case offered these observations about the serious threats to privacy that are presented by the unrestricted use of grand jury subpoenas:

> The unrestricted use of grand jury subpoenas to obtain medical records is a serious threat to privacy. There is almost no limit on what can be obtained without the knowledge or approval of any court, any grand jury, any supervisor in a prosecutor's office, or the person affected. A prosecutor's right to snoop is not limited by the seriousness of the crime—Texas grand juries may investigate any crime, including the most minor misdemeanors. Although DWI is not a minor offense, this case is a good example. This grand jury subpoena was issued for a misdemeanor offense. . . .
>
> Imagine the opportunities for political vendettas, personal revenge, and garden variety bureaucratic abuse of power. If a partisan prosecutor wanted to know if a presidential candidate of the opposite party had cancer, or was cured of it, he or she could subpoena hospital, laboratory, or physicians' records. If the leaders of the executive branch of government wanted to see who leaked the Pentagon Papers, they would not have to burglarize the office of Daniel Ellsberg's psychiatrist—a friendly prosecutor should simply subpoena the records. If a partisan prosecutor wanted to know whether a political opponent had been treated for mental illness or for a venereal disease, he or she could subpoena the opponent's medical records. Under our law, there is not requirement that a grand jury even be in session. [citation omitted] There is no advance showing required that the material subpoenaed may be relevant to an existing or contemplated investigation, or even that there be an existing or contemplated criminal investigation. Judicial authority over the process is almost totally lacking. I know of no other part of the judicial process more open to abuse.[137]

The court recommended the enactment of narrowly drafted legislation to put reasonable limits upon the use of grand jury subpoenas for things as intimate as health records. The Privacy Protection Study Commission offered similar recommendations.[138] The provisions of § 130(b) are derived from recommendations made by the Privacy Protection Study Commission. The restrictions on grand jury subpoenas will limit or eliminate abusive grand jury subpoe-

---

[135] Id. at 377.
[136] *Thurman* v. *Texas*, 861 S.W. 2d 96 (1993).
[137] Id.
[138] Id. at 378.

nas for protected health information but will not interfere with legitimate grand jury investigations.

The restrictions in section 5140(d) are intended to make sure that grand jury subpoenas are only used for legitimate grand jury purposes, to limit use of protected health information to the purpose for which the grand jury obtained it, and to require that the information be returned to the trustee or destroyed.

Most health information trustees are authorized to comply with legal process. There are three types of trustees—health information service organizations, public health authorities, and health researchers—who are not so authorized. Any protected health information in the possession of these trustees will have originated with a health care provider. Legal process for the records should be directed to the provider and not to a secondary source. For example, allowing disclosure of records in any type of central repository—like a health information service organization—may constitute a circumvention of the confidentiality interests of patients as well as of the interests of providers. Health care providers may have interests in protecting the confidentiality of their own records that overlap with or are independent of the interest of their patients. It is desirable, where practicable, for providers to be involved in requests for treatment records. This is especially true for records such as mental health treatment notes.

It is important that any such repositories not become general sources of patient information for other purposes, especially by subpoena. Exempting these trustees from complying with compulsory process will help to accomplish this. The exemption will not protect these trustees from compulsory process that is used to enforce a type of access that would otherwise be permitted under Subpart B without compulsory process.

SECTION 5141. HEALTH INFORMATION SERVICE ORGANIZATIONS

Section 5141 provides that health information trustees may disclose protected health information to a health information service organization for the purpose of permitting the organization to perform a function authorized by the Secretary. At the time that the Fair Health Information Practices Part of H.R. 3600 was approved by the Committee on Government Operations, the nature, function, and designation of health information service organizations was not yet established.[139] This section recognizes that there may be a new type of organization that will serve a function in the collection, transmission, or use of protected health information. Until the functions are set elsewhere, the terms under which information can flow cannot be defined with any precision.

SECTION 5151. ACCESS PROCEDURES FOR LAW ENFORCEMENT SUBPOENAS, WARRANTS, AND SEARCH WARRANTS

There are three different procedures for legal process under the Fair Health Information Practices Part. Section 5151 sets out the procedures for warrants and for legal process used for law enforce-

[139] See generally IOM Health Data Report (discussing the role of health database organizations).

ment purposes. Section 5153 sets out the procedures for all other legal process.

Section 5151(b) sets out the procedures that apply to judicial and administrative warrants and search warrants. Within 30 days after the date that a warrant seeking medical information is served on a health information trustee, the government authority that obtained the information must serve the patient with a copy of the warrant or must mail a copy to the last known address of the patient. No advance notice to the patient is required, and no new challenge rights are provided for warrants. This provision is not intended to override any legislation restricting the use of warrants to obtain information from third party record keepers.

The most elaborate access procedures in the bill are for administrative and judicial summonses and subpoenas issued for law enforcement purposes. These procedures are found in section 5151. The complexity is appropriate because a patient's privacy interest are most directly threatened by the possible use of protected health information against the patient in a judicial or administrative action or investigation. In addition, the occasional needs of law enforcement agencies for secrecy or dispatch in obtaining information must be accommodated.

A government authority may only obtain protected health information for use in a law enforcement inquiry through legal process if there is probable cause to believe that the information will be relevant to the inquiry being conducted by the authority. This standard was chosen because it is identical to the access standard in the Video Privacy Protection Act of 1988.[140] There is no reason why health records should receive lesser protection than video rental records.

On or before the date that the process is served on the health information trustee, the government authority must serve on the patient, or mail to his last known address, a copy of the process together with a notice of the patient's right to challenge the process. The Secretary is required to prepare a notice of patient's rights under section 5155(1), and all notices given to patients must include all of the information that is in the Secretary's notice.

If thirty days have passed from the date of service of a copy of the process upon the patient, or from the date of mailing, and no challenge has been initiated by the patient as provided in section 5152, then the government authority may obtain the protected health information from a health care trustee. If a timely challenge has been filed, then the process may only be enforced by order of a court.

With the approval of a court, the government authority may delay notifying a patient that protected health information about the patient is being sought. An application for delay must state with reasonable specificity why the delay is being sought. The court may grant the delay if (1) the inquiry is being conducted within the lawful jurisdiction of the government authority; (2) there is probable cause to believe that the information being sought will be relevant to a legitimate law enforcement inquiry; (3) the government authority's need for the information outweighs the patient's privacy

[140] 18 U.S.C. § 2710(b)(3) (1988).

interest; and (4) there are reasonable grounds to believe that receipt of a notice by the patient will result in (a) endangering the life of physical safety of any individual, (b) flight from prosecution, (c) destruction of or tampering with evidence or the information being sought, or (d) intimidation of potential witnesses.

Any court order delaying notice to the patient may also prohibit a health information trustee from revealing the request for information to the patient. Extensions of a delay order may be obtained in the same fashion as the original application. When the period of delay has expired, the government authority must serve upon the patient a copy of the process, the notice of patient rights, a copy of the application for delay, and a copy of the court order.

SECTION 5152. CHALLENGE PROCEDURES FOR LAW ENFORCEMENT SUBPOENAS

Section 5152 sets out the procedures for a challenge to a law enforcement summons or subpoena. A patient may file a challenge in an appropriate court without being required to pay any filing fee. In the case of a state judicial subpoena, the challenge may be filed in any court of competent jurisdiction.

For federal judicial subpoenas, a patient challenge may be filed in any federal court of competent jurisdiction. In most instances under the Federal Rules of Civil and Criminal Procedure, this will mean the court that issued the subpoena. For other summonses and subpoenas issued under the authority of the United States (chiefly administrative summonses), the patient may file in the United States district court for the district in which the patient resides or in which the summons or subpoena was issued, or in another United States Court of competent jurisdiction.

A patient's challenge will be in the form of a motion to quash the summons or subpoena. The patient must serve a copy of the motion upon the government authority. Once the motion to quash has been filed, the burden of going forward and the burden of justifying the process fall upon the government authority seeking the information. The government authority may respond to the motion to quash by filing with the court affidavits and other sworn documents to sustain the validity of the summons or subpoena. Within five days after the filing by the government authority, the patient may file affidavits and other sworn documents in response to the authorities filing. With the permission of the court, both parties may proceed in camera.

In deciding the motion, the court may conduct any proceeding that it deems appropriate. All proceedings should be completed and a decision rendered within ten days of the date of the government authority's filing, but the court may extend the time limits at its discretion. However, a failure of the court to rule on a motion within ten days does not operate as a denial of the motion.

A court may deny a patient's timely motion to quash if it finds that there is probable cause to believe that the law enforcement inquiry is legitimate and that the information being sought is relevant to that inquiry. Notwithstanding such a finding, a court may nevertheless grant the patient's motion if it finds that the patient's privacy interest outweighs the government authority's need for the information.

This balancing test has been included because the government's need for protected health information about a patient is not always more important than the patient's interest in the privacy of his records. When a medical record contains sensitive information about the patient, and the law enforcement inquiry does not involve a major matter or the information is not of great importance to the inquiry, a court may decide to grant the patient's motion to quash despite the relevance of the information. The burden of demonstrating that the privacy interest outweighs the government authority's need falls on the patient.

In balancing the patient's privacy interest, the court may consider (1) the particular purpose for which the information was collected by the medical care facility; (2) the degree to which disclosure of the information will embarrass, injure, or invade the privacy of the patient; (3) the effect of the disclosure of the patient's future health care; (4) the importance of the inquiry being conducted by the government authority and the importance of the information to that inquiry; and (5) any other factor deemed relevant by the court.

The balancing test may be used to deny the government authority access to some or all of the protected health information about a patient. When the disclosure of information would tend to unfairly stigmatize a patient, a judge may find it appropriate to protect the patient's interest in privacy. For example, information about psychiatric care, drug abuse or alcoholism, sexually-transmitted disease treatment, and similar matters are examples of types of data that are more sensitive and personal. On the other hand, directory information about a patient's hospital stay would in most instances be less sensitive.

If a patient files a motion to quash and substantially prevails, the court may assess against a Federal government authority attorney fees and court costs reasonably incurred by the patient. Any court ruling denying a motion to quash shall not be deemed a final order in any legal proceeding initiated against the patient arising out of or based on the protected health information disclosed.

All summonses and subpoenas for protected health information—other than law enforcement summonses and subpoenas subject to section 5151—are governed by the rules established in section 5153. This includes subpoenas issued on behalf of a government authority which is not acting in a law enforcement capacity. No person may obtain protected health information from a health information trustee unless there are reasonable grounds to believe that the information will be relevant to a lawsuit or other judicial or administrative proceeding.

SECTION 5153. ACCESS AND CHALLENGE PROCEDURES FOR OTHER SUBPOENAS

The patient notice procedures under section 5153 are essentially similar to the procedures for law enforcement subpoenas. There is, however, no provision for delay of notice. The patient may challenge a summons or subpoena issued under section 5153 by filing a motion to quash in a court of competent jurisdiction and by serving a copy of the motion of the person seeking the information.

The patient may oppose or seek to limit the summons or subpoena on any ground that would otherwise be available if the patient were in possession of the information. This would include but not necessarily be limited to the reasons for seeking a protective order listed in Rule 26(c) of the Federal Rules of Civil Procedure. These include annoyance, embarrassment, oppression, or undue burden. However, a patient may not assert the rights of a medical care facility.

The burden in these cases is different than for law enforcement subpoenas. The burden of showing reasonable grounds to believe that the information will be relevant to a lawsuit or other proceeding falls on the proponent of the subpoena. This parallels the law enforcement subpoenas section. The proponent also bears the burden of demonstrating that the need for the information outweighs the privacy interest of the individual. As a result, the proponent can be denied access even if the patient never speaks. The specific considerations to be evaluated in assessing a patient's privacy interest are virtually the same as for law enforcement subpoenas.

SECTION 5154. CONSTRUCTION OF SUBPART; SUSPENSION OF STATUTE OF LIMITATIONS

Section 5154(a) makes it clear that none of the subpoena challenge procedures affect the right of a health information trustee to challenge a request for protected health information. Trustees may have independent grounds for challenging compulsory process. At the same time, nothing is intended to entitle protected individuals to assert the rights of health information trustees.

Section 5154(b) provides if an individual challenges a government subpoena for protected health information in a manner that has the effect of delaying access by the government, any applicable statute of limitations for a civil or criminal action is extended for the period of the challenge.

SECTION 5155. RESPONSIBILITIES OF THE SECRETARY

Section 5155 provides that the Secretary of Health and Human Services shall develop notices for use under section 5151 and section 5153 that must be used to inform protected individual about their challenge rights for compulsory process.

SECTION 5161. PAYMENT CARD AND ELECTRONIC PAYMENT TRANSACTIONS

The Fair Health Information Practices Part offers comprehensive protections for identifiable health information that is generated through or becomes a part of the health care system. Most payments for health care services will be handled through insurers who are directly covered by the Part. As a result, the information disclosed to them will be fully covered by the Part's protections. However, when payments for health care services are made independently through third party payment mechanisms, there is a distinct possibility that personal health information could lose protections as payment information is processed outside the scope of the Part.

For example, when an individual pays for health services with a credit card, those engaged in processing the credit card payment acquire some information about the individual. This includes the name of the individual, the name of the physician ("merchant"),[141] the date of the transaction, and the amount of payment. While detailed information about the goods or services provided to the customer may not be included, the information that is transmitted is not trivial. The specialty of a physician can be readily determined from public sources. This may indicate the type of treatment. For example, it may be inferred that a patient of an oncologist suffers from cancer. Other inferences can be made about a patient being treated at the Betty Ford Center. Additional personal health data may be inferred from the frequency of visits and the amount of payment.

The regular compilation of health payment data over time could result in the establishment of personal health dossiers that are not subject to any legal restrictions on use or disclosure. This is not a theoretical possibility. At least one company is advertising a health care credit card dedicated to the payment of health care expenses. One of the benefits offered by this card issuer is an itemized listing of expenses that could be used for tax filing or household budgeting expenses. The unrestricted use of that same information by the card issuer could result in significant intrusions into the privacy interests of individuals.

The use of credit/debit cards for payment of health care products and services is increasing. According to Mastercard International, more physicians are requiring patients to pay for services at the time of delivery. Coinsurance is rising and deductibles are increasing as well. Mastercard's sales volume for health care exceeds two billion dollars and is increasing steadily.

It has already been documented in this report that the direct marketing industry is actively engaged in the selling of mailing lists that include specific health information about identified individuals. Some of the same type of health information that is already being bought and sold routinely could be derived from credit card and other payment system data. In order to protect the interests of individuals receiving and paying for health care, section 5161 includes specific protections against misuse of health data derived from the payment system. The intent is to create standard guidelines that will support the continued use of a variety of payment systems in the health industry without impinging on the privacy interests of patients.

Section 5161 establishes special rules for payment transactions. Trustees may disclose limited amounts of protected health information for payment purposes when an individual presents a credit card, debit card, other payment card or account number, or authorizes other electronic payment means. The presentation by the individual of a card, number, or acceptance of electronic payment is sufficient authorization for the trustee to begin the payment proc-

[141] Information provided by Mastercard International lists sixteen health care-related merchant categories, including doctors and physicians; chiropractors; dental and medical laboratories; ambulance services; hearing aid sales and service, and orthopedic goods—artificial limb stores. With this information, it is possible to make informed determinations about the general nature of health care products and services that have been provided to particular patients.

ess. There is no requirement that a formal authorization meeting the terms of section 5132 be executed.

Once the individual has initiated or agreed to one of these payment methods, the trustee is authorized to disclose only such protected health information as is necessary for the processing of the payment, for billing, or for collection. The standard information traditionally transmitted as part of a credit transaction meets this standard. This does not, however, permit the disclosure of specific protected health information by the trustee. A routine transaction would identify the patient, the service provider, the date, and the amount. The address and telephone number of the individual might be also disclosable, but only when needed for payment, billing, or collection and not otherwise prohibited by state or federal law. Details of treatment, diagnoses, medical history, and similar protected health information will not qualify for disclosure under this standard.

This disclosure authority is included in the bill because of the need to recognize the manner in which payments are normally authorized by individuals. It is an exception, albeit a limited one, to the Part's usual disclosure rules, and it should be narrowly construed. The recipients of the data (i.e., credit card processors, banks) are themselves subject to the specific rules of the credit/debit/electronic payment provisions. These recipients are not health information trustees, and they are not subject to the other requirements of the Part. Their responsibilities under the Fair Health Information Practices Part are fully described in section 5161.[142]

Subsection (b) establishes rules on use and disclosure of identifiable information obtained through payment processing. In general, the purpose is to authorize only those uses and disclosures that are "necessary" for the routine processing of payments and the conduct of the business of processing. Other uses and disclosures -- such as for direct marketing by the processor or by others, for the development of consumer profiles, for prescreening, for credit evaluation, or for other purposes—are prohibited.

Information may be used or disclosed when necessary for authorization, settlement, billing, consumer inquiries, settlement of disputes, or collection of amounts charged or debited. Authorization is an act by a merchant to communicate by telephone or electronically basic transaction information (account number, merchant identifier, transaction amount) to obtain approval to proceed with the transaction. Settlement means the process by which the merchant's bank collects funds due to the merchant from the issuing bank. Both of these processes precede the consumer billing and collection phases of the transaction.

Information may be used or disclosed when necessary for the transfer of receivables, accounts, or interest therein. This is intended to cover the range of activities that surround the sale or transfer of receipts. Information also may be used or disclosed when necessary for the audit of payment account information; for compliance with federal, state, or local laws or regulations; or for properly authorized civil, criminal or regulatory investigations by

[142] Other applicable laws, such as the Fair Credit Reporting Act, continue to apply, of course.

federal, state, or local authorities. Other uses or disclosures are prohibited.

SECTION 5162. ACCESS TO PROTECTED HEALTH INFORMATION OUTSIDE THE UNITED STATES.

The protections provided by the Fair Health Information Practices Part could be evaded if protected health information could be transferred to another jurisdiction where the information will not receive similar legal protection. There is growing international recognition that domestic fair information practices may be insufficient when personal information crosses international boundaries. For example, the 1981 Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data includes a provision that permits the assessment of the equivalency of protection for personal data in another country.[143] Also, a key provision of the draft European directive concerning the protection of individuals in relation to the processing of automated data restricts the ability of member countries to send data to other nations where data protection laws are insufficiently protective.[144]

Professor Joel Reidenberg of Fordham Law School has written about these issues:

> Because of the transnationalization of personal information processing, fair information practice rules often consider the international implications of differing standards. Transborder data flows raise legitimate concerns for national authorities of the sufficiency of foreign fair information practice rules. Problems may arise in several contexts: the differing levels of fair information practice standards; the uncertainty of applicable law; and the practical problems of implementation. The French fear of "data havens," for example, is reasonable when information processing for French companies may be structured off-shore to avoid fair information practice rules in France.[145]

In general, the United States needs to be more aware of the possibility that information about its citizens may be transferred to other countries. With the intensive use of computers for processing of personal information and the growing availability of a global information superhighway, transborder data flows must be viewed as potentially troublesome. Many companies in the business of processing personal data are multinational and may be able to maintain data in the country that offers the most corporate flexibility and the least data protection. Protections afforded by domestic laws will be undermined if personal data is maintained in other countries that do not have modern fair information practices or that otherwise serve as data havens. Data protection is not just a national problem anymore, and the international component will con-

---

[143] Council of Europe, "Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data," Art. 12 (1981), reprinted in "Data Protection, Computers, and Changing Information Practices," Hearing before the Subcomm. on Government Information, Justice, and Agriculture, House Comm. on Government Operations, 101st Cong., 2d Sess. (1990).

[144] See Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, Eur. Parl Doc. (COM 422 final-SYN 287) (1992).

[145] Reidenberg, "The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services," 60 Fordham Law Review S137 (1992) (footnotes omitted).

tinue to grow in significance as time passes, technology advances, and interconnectivity increases. The need for better coordination of data protection policies has been recognized in Europe, and the United States will eventually need to pay attention to the international side of data protection. The Fair Health Information Practices Part takes a modest first step in that direction.

Section 5162 addresses this issue. The general rule is that a health information trustee may not permit any person who is not in the United States to have access to protected health information about an individual except in specified circumstances.[146] First, information may be sent overseas if the individual has specifically consented in an authorization that meets the requirements of the Part. A general authorization is not sufficient. The authorization must specifically mention international disclosure and meet the other standards of the authorization section. When an individual seeks health care overseas, records may be transferred pursuant to this type of authorization. If a company transfers an employee overseas, health records can be sent with the consent of the employee.

Second, information may be transferred to a country if the Secretary has determined that there are fair information practices for protected health information in that country that provide protections for the subject of the information that are equivalent to the protections in the Part. Many nations—and some local jurisdictions—have passed comprehensive data protection laws that are generally equivalent to the Fair Health Information Practices Part. Foreign laws do not have to be identical to qualify under the standard. The focus is on the scope of the protections and the remedies that are provided for individuals.

These protections can be provided in a variety of ways. Even if a country does not have a comprehensive data protection law or a specific health care fair information practices law, it is still possible that the country could offer equivalent protections to indivdiuals. Consider, for example, a country that receives protected health information for processing, such as transcribing. The data is received, transcribed, and returned to the United States. If a formal legal enclave for protected health information were established, with controls that prevent the data from being used in any way while in the country, and if the data were not retained in the country except for a brief period, the Secretary might determine that the subject of the information has equivalent protection for the brief period while the data is in the country.

A trustee that seeks to rely on the "equivalent protection" section to send protected health information to another country must obtain a determination from the Secretary in advance. Notwithstanding a positive determination from the Secretary, transferring protected health information to another country does not relieve a trustee of any responsibility under the Part.

Third, protected health information may be transferred to another country if provision of access is required under a federal stat-

---

[146] Providing access to a person overseas includes actually transferring protected health information or allowing access to the information through a computer terminal. If the information is accessible through a terminal, then the international restrictions are fully applicable.

ute, treaty, or other international agreement applicable to the United States.

There are four other conditions under which the restriction on foreign access does not apply. First, protected health information may be disclosed to a foreign public health authority. Public health investigations of infectious diseases may need to extend beyond national borders. Second, disclosures that are authorized under the emergency section or under the health research section are permitted. Third, disclosures may be made under the next of kin section. There is no reason to restrict an otherwise authorized disclosure because the next of kin happens to be in another country. The same is true for directory information that can be provided to any person. The location of the recipient is not relevant. Finally, a disclosure may be made to another country if necessary for the purpose of providing for payment for health care provided to an individual. The Committee envisions that this exception may be needed when care is provided in the United States to a foreign national who is covered by a national or private health plan. Within the United States, disclosures for payment are otherwise authorized. This language does not authorize an American insurer to maintain its routine payment records in another country and to transfer the data to that country on the grounds that the transfer is necessary to provide for payment.

Some federal agencies—such as the Department of Defense—maintain health care facilities and health care records abroad. Protected health information in the possession of a federal agency remains fully subject to the Fair Health Information Practices Part wherever the records are located. As a result, the limitations on disclosure to other countries are not relevant or applicable when protected health information is accessed outside the United States but within the possession and control of a federal agency.

SECTION 5163. STANDARDS FOR ELECTRONIC DOCUMENTS AND COMMUNICATIONS

The Secretary of Health and Human Services is required to establish standards for the creation, transmission, receipt, and maintenance in electronic and magnetic form of each type of written document required or authorized under the Fair Health Information Practices Part. This authority also extends to standards for electronic signatures. In preparing the standards, the Secretary is required to consult with interested parties, including private standard-setting organizations like the American National Standards Institute. Any standards promulgated by the Secretary should be fully compatible with comparable standards in use elsewhere.

SECTION 5164. DUTIES AND AUTHORITIES OF AFFILIATED PERSONS

Section 5164 defines how the duties and authorities of a health information trustee are to be shared with affiliated persons. In general, when organizations are affiliated persons and receive protected health information from a trustee, they may use or disclose the information for a purpose that is authorized by the Fair Health Information Practices Part, for a purpose that the trustee would be authorized to engage in, and for a purpose that the trustee has authorized the affiliated person to engage in. This means, for exam-

ple, that if an affiliated person receives protected health information from a provider for benefit claims processing, the affiliate can use the information in research activities authorized by the provider and permitted under the Part. This might include quality improvement, cost containment, outcomes research and similar activities. The affiliated person would have to follow the same procedures that the trustee would be required to follow. An affiliated person could not use protected health information for purposes related to employment, credit, marketing, or other purposes unrelated to health care delivery, improvement, and payment.

A trustee is obligated to notify its affiliated person of any duties that the affiliated person is required to fulfill and of any authorities that the affiliated person is authorized to exercise. This notice defines the responsibilities of the affiliated person, who is then considered to be a health information trustee for purposes of the Fair Health Information Practices Part. This includes the enforcement provisions of the Part. An agreement with an affiliated person does not relieve a health information trustee of its duties or liabilities under the Part.

SECTION 5165. AGENTS AND ATTORNEYS

Section 5165 addresses the needs of persons who are not able to manage their own affairs, and for whom decisions are being made by others. Subsection (a) permits those acting for such an individual under State law to exercise the rights of the individual under this Act, including the rights of access and correction, and authorization to disclose.

These designations can take many forms. Individuals may execute powers of attorney under the provisions of State law for such designations. A person may be declared incompetent by a court, and a guardian appointed. In some States, there is provision for court appointment of a guardian or conservator, without a declaration of incompetence, upon the application of either the individual or of others. In some instances, courts may tailor the powers of the conservator or guardian to the particular needs of the individual. The bill authorizes action by the legal representative "to the extent authorized." To the extent that the legal representative's powers are limited with respect to records by the court decree, those limitations would have to be observed.

Subsection (b) explicitly addresses the more specialized situation of a designation by an individual of another person to make health care decisions in case of incapacity. Most States have legislation providing for designations by individuals of others to make health care decisions for them in case of incapacity, in the form of durable powers of attorney for health care, or similar instruments. The National Conference of Commissioners on Uniform State Laws has promulgated a model law in this area, the Uniform Health-Care Decisions Act.[147] The uniform law includes a provision similar to that in the bill.

Section 5165(c) addresses a problem that arises when a patient is not capable of exercising rights but has not been legally adjudicated as incompetent or does not have a legal representative for-

[147] 9 Part I U.L.A. 93 (Supp. 1994).

mally appointed. For these individuals, the right to authorize disclosures under section 5132 may be exercised by a person who holds a health care power of attorney. If no qualified person can be found after a reasonable effort, then the right may be exercised by an available attorney or next of kin. If none of these representatives can be located, the health care provider is the person of last resort. Anyone exercising the rights of a protected individual in this manner is required to act in the best interest of the individual.

SECTION 5166. MINORS

Traditionally, health care providers have looked to the parents or legal guardians of a minor child to consent to health care on the minor's behalf and to have authority over the minor's protected health information. In recent years, however, state legislatures and the courts have acted to protect health care providers from liability for treating certain minors without parental consent. This trend has resulted from the recognition that many minors are sufficiently mature to make informed decisions about their own health care and that some young people would be deterred from obtaining needed services if they were required to obtain the consent of a parent in all instances.

These recent changes in attitudes toward the medical care of minors have shaped the provisions of the Fair Health Information Practices Part dealing with the rights of minors. Section 5166 provides that all rights of patients eighteen years of age and older shall be exercised by the patient. For a patient under fourteen years of age, all rights shall be exercised through the parent or legal guardian of the patient. For those who are fourteen, fifteen, sixteen or seventeen years of age, all rights may be exercised either by the parent or by the patient. For example, a disclosure of medical information about a patient who is fifteen years old may be made with the approval of either the parent or the child.

Notwithstanding these rules, when a child of any age has the legal capacity to apply for and obtain health care without parental consent and has sought such care, the child shall exercise all rights of a patient with respect to the protected health information relating to that care. This provision is included because of the likelihood that the disclosure of confidential medical information to a parent may function as effectively as a requirement for a parental consent which may deter the young person from seeking needed health care. Determinations about the legal capacity of a minor to seek health care without the consent of the parent will continue to be made as they are now. For example, every state authorizes emancipated minors to consent to health care, although the definition of emancipation varies from State to State. Most States view marriage or economic self-sufficiency as de facto resulting in emancipation. Most States also have laws on the books permitting young people of any age to consent to care for sexually-transmitted diseases, substance abuse, and other conditions.

The most difficult decision that arises in connection with protected health information of minors involves disclosure to the parent. The person who is best able to make judgements about the advisability of such disclosure is the treating physician who knows the child, the parents and the relationship between them. Doctors

face this problem routinely today, and the Fair Health Information Practices Part does not significantly interfere with the discretion that the doctor exercises today. When all of the provisions of the bill that relate to inspection of protected health information are considered together in the context of the parent-child relationship, the result is that the treating physician has considerable discretion in disclosing or denying information to the child or to the parent.

SECTION 5167. MAINTENANCE OF CERTAIN PROTECTED HEALTH INFORMATION

Section 5167 requires each State to establish a process under which protected health information maintained by health care providers or health benefit plan sponsors who have closed will be secured. The section requires that the information be delivered to and maintained by the state or by an entity designated by the State. The underlying problem is that there are not always clear rules that apply to providers or insurers who go out of business. The requirement in section 5167 is very general, and the States may address the problem as they see fit. States with existing laws or programs may already be in compliance with the requirement. Since records of federal health care facilities are subject to the Federal Records Act and other records laws, it is not the intent of this section to bring these facilities within the jurisdiction of the States.

SECTION 5171. CIVIL ACTIONS

Section 5171 permits any individual whose rights have been violated to bring an action for equitable relief or for damages. The remedies have been carefully structured to provide real relief for those who have been injured as a result of a violation and to discourage frivolous or trivial litigation.

While civil actions are a key element in the enforcement of fair information practices, they are not a total answer. The history of privacy laws suggests that individual lawsuits are not an especially effective enforcement mechanism. While the relief provided to specific aggrieved individuals is essential to them, lawsuits are expensive and not within the reach of everyone. As a result, individual enforcement through lawsuits cannot be relied upon as the sole enforcement method.[148] In order to help fill the enforcement gap, there are also criminal penalties and administrative penalties. General oversight may also be provided by the Secretary or by other institutions (such as accreditation and licensing authorities) that oversee the health care system.

Most Western countries have established formal government authorities charged with oversight of fair information practices laws. Professor Paul Schwartz testified about some of the benefits of a data protection authority in the United States:

> A Data Protection Board would monitor data processing practices and compliance with laws, draw the attention of the legislature and the public to problems of existing laws

[148] It is also a feature of privacy lawsuits that the public nature of litigation will necessarily result in more widespread dissemination of the information deemed to be private. A plaintiff must be willing to accept broader disclosure of personal data as a necessary condition of filing suit. This is another factor that deters individuals from using available remedies and that undermines the effectiveness of private litigation in regulating unwanted conduct.

> and the need for further regulation, assist citizens seeking to protect their interests and exercise their rights, and help business in understanding national and international legal developments. By fulfilling these tasks, the data protection commission would help to ensure that public administrative bodies, the legislature, citizens and the business community remain aware and active as the conflicts generated by information technology change.[149]

Professor Schwartz also suggested that a data protection board would be able to represent American interests and assist American companies facing scrutiny by foreign data privacy authorities. There does not appear to be any federal agency that has consistently carried out this role.[150] A data protection agency could assist individuals and record keepers alike in implementing and coordinating fair information practices. The value of a data protection agency extends beyond the immediate needs of the health care system in maintaining fair information practices or in implementing the Fair Health Information Practices Part.

For civil actions authorized under the Fair Health Information Practices Part, there is a carefully drawn distinction between the remedies that are available to an aggrieved individual. Broader remedies are available when there has been a knowing violation of the law. In the case of a knowing violation, the aggrieved individual is entitled to receive a minimum damage award of $5,000. If actual damages are higher, then the individual is eligible for actual damages. There is no requirement that an individual demonstrate actual pecuniary loss or non-pecuniary damage in order to be eligible for the $5,000 award. In addition, in the case of a knowing violation, the individual may also be awarded punitive damages and attorney's fees.

In the case of a negligent violation, damages are limited to actual damages, which may include physical and mental injury and pecuniary losses. More limited remedies are appropriate when mistakes are accidental and not intentional. It can be anticipated that in some health care or health payment settings, accidental disclosures may occur from time to time. Large institutions handling vast quantities of data will make occasional errors in data handling, and errors that involve computerized records could affect many individuals. It is not the intent of the legislation to provide windfall damages to those who are not actually harmed by these errors. For example, the accidental misrouting of a computer tape containing patient information will not give rise to individual or class action lawsuits unless the plaintiffs can demonstrate actual damages.

Theoretical or incidental disclosures without identifiable harm to specific individuals will not result in awards in cases of negligent violations. However, where there are knowing or deliberate violations or where negligence is so egregious as to rise to the level of a knowing violation, then the health information trustee will be exposed to greater damages. This is a reasonable balance between the

---

[149] "H.R. 4077 Hearings" (May 4, 1994).

[150] See, e.g, Gellman, "Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," VI Software Law Journal 199, 209–212 (1993). See also Flaherty, Protecting Privacy in Surveillance Societies (1989).

need to provide effective remedies and the need to avoid costs and unnecessary litigation.

One type of improper disclosure that gave rise to considerable discussion at hearings is the deliberate leak of patient information. Rep. Nydia Velázquez testified about the effects on her and her family of the leak of very sensitive medical information during the middle of an election campaign.[151] This chilling example of a deliberate leak has occurred to others in politics, show business, and public life in general. A deliberate leak of health records is actionable through the civil remedies, and actual and punitive damages are available, along with attorney fees.

Leaks are an unfortunate feature of modern life, and computerized record systems with multiple access points can only exacerbate the possibility of leaks.[152] Every system of records that contains valuable or newsworthy information may become the source of unauthorized disclosures. There are routine leaks from government records systems containing highly sensitive classified information notwithstanding intense security and severe criminal penalties against unauthorized disclosure.

If the source of a leak is known, but the identity of the leaker is not, fixing liability can be difficult. For example, where a hospital employee leaks a patient record, it may be clear that the hospital was the source of the record although it may be impossible to identify the employee who is responsible. While it is the intent that a health information trustee should be held responsible for its own actions, there is no strict liability imposed upon trustees. A trustee is not an absolute guarantor of the confidentiality of records that it maintains. When a trustee disregards the law in a negligent or knowing manner, the trustee can be found liable for improper disclosures. If there is neither negligence nor wilful misconduct, then there is no liability.

A trustee is responsible for maintaining reasonable and appropriate administrative, technical, and physical safeguards. The security requirement is not an absolute one. No one can be held to a standard that requires absolute security. If a trustee can demonstrate that it has established appropriate safeguards, including training about fair information practices for employees and adequate supervision of employees and record systems, the trustee has a defense to an action for an improper disclosure. The individual who actually leaked the record may be found criminally or civilly liable for his or her conduct.

SECTION 5172. CIVIL MONEY PENALTIES

If the Secretary of Health and Human Services determines that a health information trustee has demonstrated a pattern or practice of failure to comply with the provisions of the Fair Health Information Practices Part, the Secretary may impose a civil money

---

[151] "H.R. 4077 Hearings" (April 20, 1994).

[152] A computerized health record system that permits access to records from anywhere in the country when emergency care is needed far from home is also likely to permit unauthorized access under other, less beneficial circumstances. There is a clear tradeoff between benefit and harm that can result from computerization and centralization of health information. This is one reason why computerized audit trails are important elements in any computerized health system. Audit trails can be effective in identifying users of data, deterring improper uses, and pinning responsibility on culpable individuals.

penalty of not more than $10,000 for each failure. This section is intended to provide means of enforcement that does not involve criminal penalties and that does not require a lawsuit by protected individuals. The Secretary will be able to encourage enforcement, especially of those provisions that may not be a likely subject of lawsuits. An example is the section that requires trustees to maintain adequate security. If the Secretary finds a general failure to provide security, the civil money penalty will offer a effective means of requiring compliance.

SECTION 5173. ALTERNATIVE DISPUTE RESOLUTION

Section 5173 requires the Secretary of Health and Human Services to develop alternative dispute resolution methods for use by individual, health information trustees, and other persons in resolving claims. The goal is to provide a more accessible and less expensive remedy. For many individuals, bringing a lawsuit seeking enforcement of privacy rights or damages for breach of privacy rights is too expensive or too complex. Disputes over access to information or amendment of information are likely only occasionally to warrant formal lawsuits. Patients and providers are likely to be better served through other dispute resolution mechanisms such as arbitration, mediation, and other forms of negotiation. The Secretary has broad authority to develop these mechanisms. The Committee encourages the use of alternative dispute resolution mechanisms developed and implemented elsewhere.

SECTION 5174. AMENDMENTS TO CRIMINAL LAW

Section 5174 amends title 18 of United States Code by adding a new chapter defining crimes that involve the use and disclosure of protected health information. The general philosophy of the criminal penalties is that basic violations are class D felonies subject to a punishment of five years in prison and a fine of up to $250,000 for individuals and $500,000 for organizations. Violations that involve the use or disclosure of protected health information for monetary gain are class C felonies subject to a punishment of ten years in prison and similar fines. Activities that violate the law include requesting or obtaining protected health information under false pretenses from a health information trustee; knowingly obtaining protected health information from a health information trustee; knowingly obtaining protected health information from a health information trustee with the intent to sell, transfer, or use the information for profit or monetary gain; knowingly selling, transferring, or using protected health information for profit or monetary gain; knowingly using or disclosing protected health information; and knowingly selling, transferring, or using protected health information.

SECTION 5181. AMENDMENTS TO TITLE 5, UNITED STATES CODE

Protected health information currently maintained by federal agencies is subject to the Privacy Act of 1974.[153] The rules set out in the Privacy Act are more general and not as rigorous as the provisions of the Fair Health Information Practices Part. Section 5181

[153] 5 U.S.C. § 552a (1988).

generally provides for exempting protected health information subject to the Fair Health Information Practices Part from most provisions of the Privacy Act. This is accomplished by requiring the head of each agency to promulgate regulations to exempt systems of records from the Privacy Act in so far as the systems contain protected health information. This approach has been selected so that the agencies will be able to review systems of records and determine which have protected health information. The Privacy Act has traditionally operated with limited exemptions for narrow categories of records, and this method will work well here. By requiring agencies to spell out the scope of the exemptions, it will be clear which records are subject to which law.

Protected health information in the possession of federal agencies is not totally exempt from the Privacy Act. For example, there is no reason to exempt these records from the Privacy Act's publication requirement. The published description of agency systems of records is a valuable public resource as well as a useful way for agencies to keep track of their activities involving personal information. Section 5181 is selective in the provisions of the Privacy Act from which protected health information may be exempted. None of the provisions of the Privacy Act that remain applicable conflicts with the requirements of the Fair Health Information Practices Part.[154]

SECTION 5191. REGULATIONS; RESEARCH AND EDUCATION

Section 5191(a) directs the Secretary of Health and Human Services to prescribe regulations to carry out the Fair Health Information Practices Part by July 1, 1996. Section 5191(b) authorizes the Secretary to sponsor research on privacy and to develop related forms and technology. Section 5191(c) authorizes the Secretary to establish education and awareness programs.

SECTION 5192. EFFECTIVE DATES

Section 5192 establishes the effective dates for the Fair Health Information Practices Part. The basic provisions will take effect on January 1, 1997.

SECTION 5193. APPLICABILITY

This section provides transition rules that apply to protected health information and to patient authorizations in existence on the effective date.

SECTION 5194. RELATIONSHIP TO OTHER LAWS

The general policy in section 5194 is that most provisions of the Fair Health Information Practices Part are preemptive, and that State laws that are inconsistent or that impose additional requirement with respect to duties of health information trustees under

[154] The Freedom of Information Act, 5 U.S.C. §552 (1988), provides a mechanism that permits any person to request a copy of any federal record. Under the FOIA's privacy exemption, medical records have always been recognized as exempt. The passage of the Privacy Act of 1974 only reinforced the confidentiality of federal health records. In case there is any doubt, it is the intent of the Committee that the Fair Health Information Practices Part is a statute within the meaning of the third exemption of the FOIA. The legal effect is to prevent the disclosure of protected health information by a federal agency under the FOIA.

subpart A, authority to disclose under subpart B, access procedures and challenge rights under subpart C, miscellaneous provisions under subpart D, or enforcement under subpart E.

A principal exception to the preemption policy is found in section 5194(b). A state law regarding public health or mental health that prohibits or regulates a disclosure of protected health information is not superseded by the Fair Health Information Practices Part. In essence, any stricter state disclosure law remains valid in so far as it applies to public health or mental health records.

Section 5194(c) expressly provides that States may establish and enforce criminal penalties with respect to a failure to comply with a provision of the Fair Health Information Practices Part. States are encouraged to undertake enforcement of the provisions of the Part.

Section 5194(d) preserves any privileges—such as the physician patient privilege—that may exist at the state or federal level. The policy is that disclosures of protected health information—such as to insurers, for treatment, or for oversight—should not be treated as interfering with these existing privileges. Similarly, if a patient authorizes disclosure of protected health information for the purpose of receiving or paying for health care, that act does not waive any existing privilege

Section 5194(e) provides a special use and disclosure rule for the Department of Veterans Affairs. Health care and other benefit programs operated by the Department are intertwined, and the limitations in the Part would result in significant and unnecessary disruption. This provision allows for exchange of protected health information within the Department in connection with benefit programs.

Section 5194(f) makes it clear that the Fair Health Information Practices Part does not preempt, supersede, or modify—

(1) any law that provides for the reporting of vital statistics such as birth or death information;

(2) any law requiring the reporting of abuse or neglect information about any individual, including but not limited to child abuse information;

(3) subpart II of part E of title XXVI of the Public Health Service Act relating to notification of emergency response employees of possible exposure to infectious disease;

(4) the Americans with Disabilities Act of 1990; and

(5) any federal or state statute that establishes a privilege for records used in health professional peer review activities.

This list of unaffected statutes is intended to remove any doubt about the effects of the Fair Health Information Practices Part on existing laws. The list should not be read to suggest that statutes not included are automatically either superseded or are not superseded. The effect on other laws should be evaluated on a case by case basis.

For example, some information covered by this bill will continue to be covered by other Federal confidentiality statutes, and this bill is not intended to modify those statutes. If a hospital discloses information to the National Center for Health Statistics for research purposes under the procedures in section 5136, NCHS is constrained both by the use and redisclosure provisions in subsection

(c) as well as by the Center's own confidentiality statute, section 308(d) of the Public Health Service Act.[155] The bill's restrictions and restrictions under section 903(c) of the Public Health Service Act[156] would both apply if the information is disclosed to the Agency for Health Care Policy and Research or its grantees. Likewise, identifiable information received from a health information service organization by a health researcher who has protection for the identity of research subjects under section 301(d) of the Public Health Service Act,[157] is protected both by section 301(d) and by the restrictions in this bill.

Subsection 5194(f) addresses the effect of the Fair Health Information Practices Part on existing federal drug and alcohol laws. There are many areas in which the drug and alcohol laws offer protections that go beyond the provisions of the Fair Health Information Practices Part and the needs of other medical consumers in order to meet the special needs of patients of alcohol and drug treatment facilities. At the same time, there are some provisions in the Fair Health Information Practices Part that offer stronger protections.

Examples of provisions from the alcohol and drug abuse regulations that are more reflective of the needs of special needs are the patient consent requirements. As the Legal Action Center pointed out,[158] the uses of consent forms in alcohol and drug abuse program settings are different from other medical settings in ways that allow them to be more successful. Alcohol and drug abuse treatment programs and their clients are linked in common cause to protect privacy so that clients feel it is safe to obtain treatment. The consent forms required by the regulations[159] are much more specific than the normal medical release form. It is apparent that the different approach to patient consent in the Fair Health Information Practices Part will not work in the alcohol and drug treatment context. Similarly, the next of kin disclosure rules in the Fair Health Information Practices Part are not appropriate for the special needs of alcohol and drug abuse treatment.

Another area in which the alcohol and drug abuse rules clearly offer stronger protection is in the area of law enforcement and criminal justice. Law enforcement inquiries are much more sharply regulated as are rules about responding to subpoenas and search warrants. While these stricter rules may not be needed in other medical treatment settings, they are clearly appropriate for alcohol and drug abuse treatment.

The Fair Health Information Practices Part does improve upon the alcohol and drug abuse rules in several ways. Duty to warn disclosures are defined more clearly under section 5137 than under the alcohol and drug abuse rules. Also, the civil and criminal sanctions for breach of the Fair Health Information Practices Part are stronger.

---

[155] 42 U.S.C.A. 242m(d) (West Supp. 1994).
[156] 42 U.S.C.A. 299a–1 (West Supp. 1994).
[157] 42 U.S.C.A. 241 (West Supp. 1994).
[158] See testimony Susan Jacobs, Staff Attorney, Legal Action Center, in H.R. 4077 Hearings (May 5, 1994). The Legal Action Center specializes in policy and legal issues in the intersecting areas of drug and alcohol abuse and AIDS.
[159] 42 C.F.R. Part 2 (1993).

In order to meld the Fair Health Information Practices Part with the existing drug and alcohol rules, section 5194(g) provides that no provision of the Part preempts, supersedes, or modifies the operation of section 543 of the Public Health Service Act except to the extent that the Secretary of Health and Human Services determines through regulations that the Fair Health Information Practices Part provides greater protection for protected health information and for the rights of protected individuals than is provided under that section. There is a similar provision that gives the Secretary of Veterans Affairs the same authority with respect to 38 U.S.C. § 7332. The result intended by the Committee is to provide alcohol and drug abuse records with the strongest protections for protected health information and for protected individuals that can be found in either law.

Report on Section 5401 of Title V

PURPOSE AND SUMMARY

The purpose of this amendment is to prevent and detect fraud and abuse in the provision of health care.

The amendment provides for improved coordination—including the sharing of data—both among Federal law enforcement agencies and between the Federal agencies and the State agencies enforcing the Federal health fraud and abuse provisions. The amendment also provides a new source of funds for these Federal and State law enforcement agencies: a special fund comprised of fines, penalties, damages, and proceeds from forfeitures collected from those who violate Federal health fraud and abuse provisions. This special fund can be used by Federal and State law enforcement agencies to supplement regularly appropriated funds in combatting health care fraud and abuse.

BACKGROUND AND NEED FOR LEGISLATION

A. Introduction

The Committee finds that fraud, waste, and abuse are flourishing in the nation's health care industry. This fraud, waste, and abuse has serious consequences. The American Medical Association, for example, testified "The fraudulent and abusive schemes that, unfortunately, have become so prevalent in our health care system often lead to the rendering of medically unethical or potentially harmful testing, as well as inaccurate, misleading, and false diagnoses. As a consequence, such practices undermine health care delivery and have future patient and societal ramifications by generating unnecessary fear, jeopardizing the ability to obtain universal health care coverage in the future, and increasing the already high cost of health care."

The Committee concludes that necessary improvements in combatting health care fraud and abuse include better coordination of Federal and State law enforcement efforts, more resources devoted to Federal and State law enforcement, and enhancement of the nation's current health information system.

B. Scope of health care fraud and abuse

Witnesses testified that fraud, waste, and abuse constitute between three and ten percent of current expenditures on health care in the United States. This would mean that the annual cost of health care fraud, waste, and abuse is between $30 billion and $100 billion.

Some health care fraud is national. For example, in June 1994 National Medical Enterprises, Inc. ("NME") agreed with the Department of Justice ("DOJ") to pay $379 million in criminal fines, civil damages, and penalties to the Federal government and several States for kickbacks and fraud at NME psychiatric and substance abuse hospitals in more than 30 states. As another example, National Health Laboratories, Inc. ("NHL"), one of the nation's largest clinical laboratories, agreed with the DOJ in December 1992 to pay $110.5 million to settle claims that it had over-charged Medicare and 33 State Medicaid programs for certain laboratory blood tests.

Other health care fraud is local, involving, for example, false bills submitted by a single chiropractor, dentist, durable medical equipment firm, hospital, nursing home, pharmacist, physician, podiatrist, or transportation company.

C. Types of health care fraud and abuse

The Committee finds that the nature of health care fraud and abuse are generally different for "fee-for-service" and "prepaid" health care providers. According to the General Accounting Office ("GAO"), in a fee-for-service health system fraud and abuse include overcharging payers for services provided, charging for services not rendered, accepting bribes or kickbacks for referring patients, and rendering unnecessary services. In contrast, fraudulent or abusive practices found among prepaid health plans involve avoiding expensive treatments, underfinancing health plan operations, disregarding member complaints, providing poor-quality care, and using deceptive marketing practices.

D. Current efforts at preventing health care fraud and abuse

1. Activities of Major Federal Agencies

Three Federal agencies—which in fiscal year 1993 spent about $257 billion on health care—now investigate fraud, waste, and abuse in the health care programs for which they are responsible. The Inspector General of the Department of Health and Human Services ("HHS") investigates fraud and abuse in three programs: the Medicare program (which last year spent about $145 billion to cover about 35 million people), the Medicaid program (which last year spent about $81 billion in Federal funds to cover about 24 million people), and the Indian Health Service (which last year spent about $2 billion to cover about one million people). The Inspector General of the Department of Defense ("DOD") investigates fraud and abuse in the Civilian Health and Medical Program of the Uniform Services ("CHAMPUS") (which last year spent about $5 billion to cover about seven million persons) and medical care for military personnel (which last year spent about $9 billion to cover about 2 million persons). The Inspector General of the Department of Veterans Affairs ("VA") investigates fraud and abuse in the VA's

health system (which last year spent about $15 billion to cover about three million persons).

The Inspector General of the Department of Labor ("DOL") investigates bogus companies that purport to sell health insurance to unions and small companies.

Each of these four Inspectors General conducts his or her investigations under both the Inspector General Act of 1978, 5 USC App. 3, and the Program Fraud Civil Remedies Act of 1986, 31 USC sec. 3801 et seq.

The HHS Inspector General has additional powers, under specific Medicare and Medicaid legislation, to bring an administrative action to exclude health care providers and to impose civil monetary penalties. 42 USC sec. 1320a–7 and 1395dd. For example, during the six month period April 1, 1993 to September 30, 1993 the HHS Inspector General excluded over 500 individuals and entities and recouped about $123 million because of illegitimate Medicare and Medicaid claims. The Committee is concerned that frequently the Federal government merely imposes monetary penalties rather than requiring incarceration of those who have defrauded the Federal health care system.

In addition to the Inspectors General, the Department of Justice both investigates (using the Federal Bureau of Investigation) and prosecutes criminal and civil cases in the area of health care fraud and abuse.

2. State and private activities

State governments are also concerned about fraud and abuse in health care. State governments investigate and prosecute fraud and abuse in the Medicaid system (on which States spent about $60 billion in fiscal year 1993); the Federal government pays 75 to 90 percent of the costs the State Medicaid Fraud Control Units. State insurance commissioners investigate health insurance fraud and abuse.

Private insurance companies and companies that self-insure health care may also investigate fraud and abuse in the health care system. Their efforts are hampered, however, according to GAO, because of legal problems in sharing information and a lack of effective legal remedies.

3. Federal resources now devoted to combatting health care fraud and abuse

To prevent health care fraud and abuse the Federal government is spending only about one tenth of one percent of what it spends on health care. Most of the approximate $300 million spent by the Federal government to combat health care fraud and abuse is spent by HHS, which in fiscal year 1993 spent about $243 million, including about $40 million in the HHS Inspector General's office, about $58 million to partially finance State Medicaid Fraud Control Units, and about $145 million paid to 40 private companies that process Medicare claims to help detect both medically unnecessary treatment and fraudulent claims. The VA Inspector General spends about $9 million on health care fraud and abuse; the DOD Inspector General spends about $6 million, and the Department of Labor Inspector General spends about $3 million. The Federal Bureau of

Investigation is spending about $20–30 million a year investigating health care fraud.

The Federal government recovers more in health fraud cases than it spends investigating them. In fiscal year 1993 the Department of Justice, HHS Inspector General, DOD Inspector General, and VA Inspector General together recovered about $438 million in fraudulent payments in Federal health programs, as compared to less than $100 millon spent by them in combatting health care fraud.

However, in recent years there has been no significant increase in the amount of Federal resources devoted to combatting health care fraud and abuse. GAO testified that "public funding for health care enforcement activities has not keep pace with the growth in health care expenditures. For example, the number of HHS Inspector General investigators has actually declined over the past 5 years, although the Inspector General's statutory responsibilities and the size and complexity of the federal programs that the Inspector General investigates have increased significantly."

HEARINGS

The Subcommittee on Human Resources and Intergovernmental Relations held two oversight hearings in this Congress on health care fraud and abuse.

On August 2, 1993 the Subcommittee held an oversight hearing on prescription drug diversion in the Medicaid program. The witnesses at this hearing were: the Honorable Charles B. Rangel; Leslie Aronovitz, Associate Director, Health Financing Issues, General Accounting Office; Shirah Neiman, Deputy United States Attorney, Southern District of New York; Thomas F. Staffa, Chief of the Criminal Division, Office of the New York State Special Prosecutor for Medicaid Fraud Control; and Beth Taylor, Director Texas Medicaid Fraud Control Unit, Office of the Attorney General.

On February 25, 1994 the Subcommittee held an oversight hearing on Medicaid fraud in Florida. The witnesses at this hearing were: Leslie G. Aronovitz, Associate Director, Human Resources Division, General Accounting Office; Rufus D. Noble, Inspector General, Florida Agency for Health Care Administration; John Morris, Director, Florida Medicaid Fraud Control Unit; Yaakov "Jack" Kronfeld, President, Genesis Health Care; Robert Palenzuela, Chief Operating Officer and General Counsel, Community Medical Plan, Inc.; and Marshall Kelley, Director of Medicaid, Florida Agency for Health Administration.

On March 17, 1994 the Subcommittee on Legislation and National Security and the Subcommittee on Human Resources and Intergovernmental Relations held a joint legislative hearing on the fraud and abuse provisions in H.R. 3600. The witnesses at this hearing were: Leslie G. Aronovitz, Associate Director, Health Financing, General Accounting Office; the Honorable Derek J. Vander Schaaf, Deputy Inspector General of the Department of Defense; the Honorable June Gibbs Brown, Inspector General of the Department of Health and Human Resources; the Honorable Charles C. Masten, Inspector General of the Department of Labor; the Honorable Stephen A. Trodden, Inspector General of the Department of Veterans Affairs, Gerald M. Stern, Special Counsel for

Financial Institution Fraud, Department of Justice; William W. Whatley, Jr., Alabama Deputy Attorney General, President, National Association of Medicaid Fraud Control Units; David J. Lyons, Iowa Commissioner of Insurance, Vice President, National Association of Insurance Commissioners; William J. Mahon, Executive Director, National Health Care Anti-Fraud Association; and Dr. Jerald R. Schenken, Member, Board of Trustees, American Medical Association.

COMMITTEE CONSIDERATION

On July 27, 1994 the Subcommittee on Human Resources and Intergovernmental Relations, a quorum being present, approved by voice vote an amendment offered by Mr. Towns and Mr. Schiff to section 5401. Mr. Schiff then offered an amendment providing that in the case of a Federal health care offense, the attorney for the government may not, in exchange for payment by a defendant of any monetary amount, reduce the exposure of the defendant to a term of imprisonment by moving for dismissal or reduction of charges. Mr. Towns, while indicating general support for the intent of the amendment, said it was not germane, and Mr. Schiff withdrew the amendment.

On July 27, 1994 the Committee on Government Operations, a quorum being present, approved by voice vote the amendment as reported by the Subcommittee and ordered the amendment reported.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

Subsection (a) of the amendment provides for Federal efforts by Inspectors General and the Attorney General to prevent and detect health care fraud and abuse. The subsection authorizes six Federal officials—the Inspector General of the Department of Health and Human Services ("HHS"), the Inspector General of the Department of Defense ("DOD"), the Inspector General of the Department of Labor ("DOL"), the Inspector General of the Office of Personnel Management ("OPM"), the Inspector General of the Department of Veterans Affairs ("DVA"), and the Attorney General—to prevent, detect, and control health care fraud and abuse in violation of any Federal law. However, the Inspectors General other than the Inspector General of HHS may not investigate health care fraud and abuse under various titles of the Social Security Act. The Committee intends that the Inspectors General, in carrying out these responsibilities, may exercise all the powers available under the Inspector General Act of 1978 even if the fraud and abuse does not involve Federal funds.

Each of these six Federal officials is to prepare an annual investigative plan for the prevention, detection, and control of health care fraud and abuse and to consult with each other and with other Federal, State, and local law enforcement agencies and agencies responsible for the licensing and certification of health care providers.

The Inspector General of HHS and the Attorney General are jointly to establish by January 1, 1996 a program to coordinate the activities of Federal, State, and local law enforcement agencies and Federal and State agencies responsible for licensing and certifying

health care providers in preventing, detecting, and controlling health care fraud and abuse. A description of this program shall be published in the Federal Register by June 30, 1995.

Subsection (b) of the amendment provides for State prevention, detection, and control of health care fraud and abuse in violation of any Federal law. The Governor of each State, consistent with State law, is to designate State agencies which shall prevent, detect, and control health care fraud and abuse within the State that violates any Federal law. One of these agencies is to be designated as the lead agency for the State.

The amendment also provides that a State may establish a State Health Care Fraud Control Unit ("Fraud and Abuse Unit"), modeled after existing Medicaid Fraud Control Units. The amendment includes the criteria which must be met by the Fraud and Abuse Unit, including its separation from any State agency responsible for administering any Federally funded or mandated health care program and the authority to prosecute individuals for criminal violations or assist in such prosecutions. The Committee expects that in most cases the lead agency for the State will be the Medicaid Fraud Control Unit created pursuant to 42 U.S.C. 1396b(q).

Each State's Fraud and Abuse Unit may submit each year to the Inspector General of HHS and the Attorney General a plan for preventing, detecting, and controlling health care fraud and abuse in the State that is consistent with the Federal plan for preventing, detecting, and controlling health care fraud and abuse. The Inspector General of HHS shall approve the plan unless the Inspector General establishes that the State plan is inconsistent with the Federal plan or will not enable the State agencies to prevent, detect, and control health care fraud and abuse. Each Fraud and Abuse Unit shall submit an annual report to the Inspector General of HHS.

The Inspector General of HHS shall report to Congress twice a year on how well the States are preventing, detecting, and controlling health care fraud and abuse.

Subsection (c) of the amendment provides that for those States which have established a Fraud and Abuse Unit and for which an annual plan has been submitted and approved, the Inspector General of HHS shall pay each State agency—subject to availability of appropriations—an amount equal to 75 percent of the agency's costs in combatting health care fraud and abuse.

Subsection (d) of the amendment directs the Inspector General of HHS and the Attorney General to establish a program for the sharing among Federal, State, and local law enforcement agencies and health care providers and insurers of data related to possible health care fraud and abuse.

Subsections (e) through (h) of the amendment establish a Health Care Fraud and Abuse Enforcement Control Account ("the Account") to help pay for the Federal and State costs of preventing and controlling health care fraud and abuse. The Account has an expenses subaccount and a reserve subaccount. Into the expenses subaccount are deposited: (1) all fines for health care fraud and abuse, (2) civil penalties and damages (other than restitution) for false claims based on health care fraud and abuse, (3) administrative penalties under the Social Security Act, (4) proceeds of seizures

and forfeitures of property in connection with health care fraud and abuse in violation of any Federal law, and (5) donations. Once the expenses subaccount reaches $500 million, it cannot grow by more than 10 percent per annum. Sums in excess of this ceiling are deposited into the reserve subaccount until it reaches 10 percent of the amount in the expenses subaccount. Additional sums are to be transferred to the general fund of the Treasury. Funds from the reserve subaccount can be transferred to the expenses subaccount in a particular year so that expenditures from the expenses subaccount do not fluctuate widely.

The HHS Inspector General and the Attorney General are jointly to use the funds in the expenses subaccount to pay their expenses and the expenses of other Inspectors Generals and Federal, State, and local agencies in connection with their prevention and detection of health care fraud and abuse. A State or local law enforcement agency is to receive an amount from the expenses subaccount that reflects generally and equitably the contribution of that agency to the deposits made into the expenses subaccount.

Amounts received from the expenses subaccount are to supplement regularly appropriated funds for these Federal agencies.

An Account Payments Advisory Board ("the Board") is established to make recommendations to the HHS Inspector General and the Attorney General regarding the equitable allocation of amounts in the Account. The Board is comprised of four Federal officials—the Inspector General of the DOD, the Inspector General of the DOL, the Inspector General of the OPM, and the Inspector General of the DVA—and ten members appointed by the Inspector General of HHS to represent State law enforcement agencies, with one member being appointed from each of the ten regions of the country established by the Office of Management and Budget from among persons recommended by the heads of those State law enforcement agencies designated by the Governors in each region.

Subsection (i) of the amendment defines the terms "account," "expenses subaccount," "health care fraud and abuse control unit," "Inspector General," and "reserve subaccount."

Subsection (j) gives the effective dates of section 5401.

Committee Oversight Findings

Pursuant to clause 2(l)(3)(A) and clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives, the Committee held oversight hearings and made findings that are reflected in the legislation and in this report.

Committee Cost Estimate

Pursuant to clause 7(a) of rule XIII of the Rules of the House of Representatives, the Committee makes the following estimate of the costs of carrying out these amendments for fiscal year 1994 and for the succeeding five fiscal years. The Committee estimates that enactment of the Fair Health Information Practices Part will have no net cost to the Federal government and may actually save money by establishing uniform rules and by supporting the use of more efficient computer and telecommunication technology for the transfer of health information. The Committee also estimates that

the amendment to section 5401 of title V will have no net cost to the Federal government and will actually save the Federal government money, since the sums spent each year by the Federal government in preventing and detecting health care fraud and abuse are substantially less than the repayments made to the Federal government by those who are caught defrauding the Federal government.

Inflationary Impact Statement

Pursuant to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the Committee makes the following statement with regard to the inflationary impact of the amendments: the amendment adding the Fair Health Information Practices Part will not have an inflationary impact because it will likely reduce costs by establishing uniform rules and by supporting the use of more efficient computer and telecommunication technology for the transfer of health information; and the amendment to section 5401 of title V will not have an inflationary impact because it will reduce the amount of fraud and abuse in the delivery of health care.

Changes in Existing Law Made by the Bill, as Reported

Pursuant to the terms of the referral of the bill to the Committee, the Committee adopted amendments to subtitle B of title V and section 5401.

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the portions of the bill to which amendments were adopted by the Committee, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

CHAPTER 90—PROTECTED HEALTH INFORMATION

§1831. Definitions

As used in this chapter—

(1) the term "health information trustee" has the meaning given such term in section 5120(b)(6) of the Health Security Act;

(2) the term "Protected health information" has the meaning given such term in section 5120(a)(3) of such Act; and

(3) the term "protected individual" has the meaning given such term in section 5120(a)(4) of such Act.

§1832. Obtaining protected health information under false pretenses

Whoever under false pretenses—

(1) requests or obtains protected health information from a health information trustee; or

(2) obtains from a protected individual an authorization for the disclosure of protected health information about the individual maintained by a health information trustee;

shall be fined under this title or imprisoned not more than 5 years, or both.

§1833. Monetary gain from obtaining protected health information under false pretenses

Whoever under false pretenses—

(1) requests or obtains protected health information from a health information trustee with the intent to sell, transfer, or use such information for profit or monetary gain; or

(2) obtains from a protected individual an authorization for the disclosure of protected health information about the individual maintained by a health information trustee with the intent to sell, transfer, or use such authorization for profit or monetary gain;

and knowingly sells, transfers, or uses such information or authorization for profit or monetary gain shall be fined under this title or imprisoned not more than 10 years, or both.

§1834. Knowing and unlawful obtaining of protected health information

Whoever knowingly obtains protected health information from a health information trustee in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such obtaining is unlawful, shall be fined under this title or imprisoned not more than 5 years, or both.

§1835. Monetary gain from knowing and unlawful obtaining of protected health information

Whoever knowingly—

(1) obtains protected health information from a health information trustee in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such obtaining is unlawful and with the intent to sell, transfer, or use such information for profit or monetary gain; and

(2) knowingly sells, transfers, or uses such information for profit or monetary gain;

shall be fined under this title or imprisoned not more than 10 years, or both.

§1836. Knowing and unlawful use or disclosure of protected health information

Whoever knowingly uses or discloses protected health information in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such use or disclosure is unlawful, shall be fined under this title or imprisoned not more than 5 years, or both.

§1837. Monetary gain from knowing and unlawful sale, transfer, or use of protected health information

Whoever knowingly sells, transfers, or uses protected health information in violation of part 2 of subtitle B of title V of the Health Security Act, knowing that such sale, transfer, or use is unlawful, shall be fined under this title or imprisoned not more than 10 years, or both.

* * * * * * *

SECTION 552a OF TITLE 5, UNITED STATES CODE

§ 552a. Records maintained on individuals

(a) * * *

* * * * * * *

(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

(1) * * *

* * * * * * *

(3) establish procedures for the disclosure to an individual upon his request of his record or information [pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records pertaining to him;] *pertaining to the individual;*

* * * * * * *

(w) MEDICAL EXEMPTIONS.—The head of an agency that is a health information trustee (as defined in section 5120(b)(6) of the Health Security Act) shall promulgate rules, in accordance with the requirements (including general notice) of subsections (b)(1), (b)(2), (b)(3), (c), and (e) of section 553 of this title, to exempt a system of records within the agency, to the extent that the system of records contains protected health information (as defined in section 5120(a)(3) of such Act), from all provisions of this section except subsections (e)(1), (e)(2), subparagraphs (A) through (C) and (E)

through (I) of subsection (e)(4), and subsections (e)(5), (e)(6), (e)(9), (e)(12), (l), (n), (o), (p), (q), (r), and (u).

○

82-256 O - 94 (168)